UNIVERSIDADE TÉCNICA DE LISBOA
INSTITUTO SUPERIOR DE ECONOMIA E GESTÃO

SISTEMAS DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL EM INSTITUIÇÕES FINANCEIRAS

Tese apresentada e defendida por Rui Alexandre Henriques Gonçalves perante o Júri abaixo designado para a obtenção do grau de Doutor em Gestão pelo Instituto Superior de Economia e Gestão da Universidade Técnica de Lisboa.

Presidente
Reitor da Universidade Técnica de Lisboa

Vogais
Doutor António Maria Palma dos Reis, orientador, professor Catedrático do Instituto Superior de Economia e Gestão da Universidade Técnica de Lisboa;
Doutor Fernando José Ferreira Lucas Bação, professor associado do Instituto Superior de Estatística e Gestão de informação da Universidade Nova de Lisboa;
Doutor Mohamed Azzim Gulamhussen, professor associado do Departamento de Finanças e Contabilidade do Instituto Superior de Ciências do Trabalho e da Empresa;
Doutor Eduardo Barbosa do Couto, professor auxiliar do Instituto Superior de Economia e Gestão da Universidade Técnica de Lisboa;
Doutor Jorge Humberto da Cruz Barros de Jesus Luís, professor auxiliar convidado do Instituto Superior de Economia e Gestão da Universidade Técnica de Lisboa.

Lisboa, Abril de 2011

UNIVERSIDADE TÉCNICA DE LISBOA
INSTITUTO SUPERIOR DE ECONOMIA E GESTÃO

SISTEMAS DE INFORMAÇÃO PARA GESTÃO DE RISCO OPERACIONAL EM INSTITUIÇÕES FINANCEIRAS

Tese apresentada e defendida por Rui Alexandre Henriques Gonçalves perante o Júri abaixo designado para a obtenção do grau de Doutor em Gestão pelo Instituto Superior de Economia e Gestão da Universidade Técnica de Lisboa.

Presidente
Reitor da Universidade Técnica de Lisboa

Vogais
Doutor António Maria Palma dos Reis, orientador, professor Catedrático do Instituto Superior de Economia e Gestão da Universidade Técnica de Lisboa;
Doutor Fernando José Ferreira Lucas Bação, professor associado do Instituto Superior de Estatística e Gestão de informação da Universidade Nova de Lisboa;
Doutor Mohamed Azzim Gulamhussen, professor associado do Departamento de Finanças e Contabilidade do Instituto Superior de Ciências do Trabalho e da Empresa;
Doutor Eduardo Barbosa do Couto, professor auxiliar do Instituto Superior de Economia e Gestão da Universidade Técnica de Lisboa;
Doutor Jorge Humberto da Cruz Barros de Jesus Luís, professor auxiliar convidado do Instituto Superior de Economia e Gestão da Universidade Técnica de Lisboa.

Lisboa, Abril de 2011

Resumo

As áreas de risco de mercado e de crédito são alvo de análises sofisticadas desde há vários anos por parte das instituições financeiras, mas estas só recentemente se aperceberam da importância do risco operacional. Este trabalho tem como principal objectivo fornecer uma perspectiva do estado presente do desenvolvimento da gestão de risco operacional em instituições financeiras, evidenciando algumas limitações dos sistemas actuais e apresentando uma arquitectura que permita a promoção de sistemas de informação que proporcionem a instituições financeiras e reguladores um suporte que os apoie na tomada de decisão na área do risco operacional. A metodologia de investigação utilizada assenta na revisão da literatura; num questionário realizado a um conjunto de instituições bancárias e seguradoras portuguesas, bem como às entidades reguladoras destes sectores. Com base na análise dos requisitos identificados, foi utilizada a *Soft System Methodology* para o desenho conceptual de um sistema de informação para o risco operacional que possa responder às necessidades actuais e futuras das instituições financeiras em Portugal.

JEL Codes: C88, E58, G21, G22, G32.

Palavras-chave: Risco Operacional; Instituições Financeiras; Sistemas de Informação.

Abstract

Market and credit risk have been subject to sophisticated analysis by financial institutions since many years. But only recently those institutions realized the importance of operational risk. This work's main objective is to supply a broad vision of operational risk management late development in financial institutions, putting in evidence some of the limitations of the systems in place, and to present an information systems architecture able to supply the financial institutions and regulators, a framework that supports decision making for operational risk. The investigation methodology is built on literature revision, and a questionnaire presented to a set of Portuguese banking and insurance institutions, as well as to the regulators of these sectors. With these set of requisites identified, the *Soft System Methodology* is used to build a conceptual design of an information system for operational risk able to answer to Portuguese financial institutions present and future needs.

JEL Codes: C88, E58, G21, G22, G32.

Keywords: Operational Risk, Financial Institutions, Information Systems.

Agradecimentos

Quero agradecer em primeiro lugar à minha mulher, Rute, pela motivação, muita paciência, e todo o apoio que foram fundamentais para a conclusão deste trabalho. Quero também agradecer aos meus pais por todo o apoio, que sem o qual não teria sido possível embarcar neste projecto.

Um agradecimento muito especial ao Prof. Palma dos Reis, cuja orientação foi determinante em momentos críticos do desenvolvimento da tese.

Quero agradecer a todos os colegas, e amigos, que durante o período da tese me ajudaram, quer através das críticas e sugestões, ou apenas pelas palavras de confiança.

Um agradecimento especial para a Lena Antunes que foi a força que me “obrigou” a começar, e a acabar, este projecto.

Índice

Índice de Figuras

I Parte – OBJECTIVOS E RELEVÂNCIA

1 – INTRODUÇÃO

O risco operacional não constitui novidade: é o mais antigo risco que as instituições financeiras enfrentam. Apesar da sua constante presença em todas as actividades de uma instituição financeira, têm sido as áreas de risco de mercado e de crédito os alvos principais de análises sofisticadas e robustas desde há vários anos. Só recentemente as instituições financeiras se aperceberam da relevância do risco operacional (Bessis 2002). Razões como a sua difícil identificação e medição e a ausência da devida atenção por parte do mercado e reguladores concorreram para que o foco na sua análise e gestão tenha sido negligenciado até ao final da década de 90. No entanto, vários determinantes vêm contribuindo para a crescente importância concedida ao risco operacional (Geiger 2000): (i) a percepção do crescimento do impacto dos riscos operacionais; (ii) a constatação da insuficiência do recurso a abordagens somente quantitativas de risco de crédito e de mercado para captar alguns tipos de risco e o reconhecimento de que a gestão de risco operacional deve ser uma disciplina por direito; (iii) a inclusão dos riscos operacionais nas metodologias de gestão global de risco e (iv) o interesse crescente das entidades reguladoras pelo risco operacional ao nível dos requisitos de capital e da sua gestão.

O risco operacional pode ser definido como o risco resultante da materialização de uma vasta diversidade de eventos, incluindo fraude, roubo, perda de membros-chave da equipa, processos judiciais, perda de informação, terrorismo, vandalismo e desastres naturais. De acordo com Brink (2002), números recentes apontam para valores elevados (entre 400 e 2850 milhões de dólares) nas perdas resultantes deste tipo de risco, embora o autor afirme que estes valores representam apenas uma pequena parte do volume total das perdas que têm por base o risco operacional das diferentes instituições. A

divulgação destes números, bem como o surgimento constante de escândalos financeiros (e.g. Enron, Parmalat e Société Générale), sem esquecer o facto de as perdas resultantes de eventos operacionais se encontrarem na base dos mais espectaculares falhanços empresariais (Barings, Long Capital Management), levam a que o risco operacional tenha vindo a receber progressivamente mais atenção por parte da comunicação social, de reguladores e gestores executivos. Para fazer face a esta realidade, as entidades reguladoras têm investido em apresentar novas normas e regras das quais são exemplos os Acordos Basileia II e Solvência II, visando, respectivamente, a área da banca e a área seguradora (Saidenberg et al. 2003).

Jobst (2007) aponta a desregulamentação dos mercados financeiros, a crescente complexidade da indústria financeira, as grandes fusões e aquisições e o recurso massivo a contractos de *outsourcing* como factores preponderantes para o aumento da exposição das actividades das instituições financeiras ao risco operacional. Também a tendência para uma maior dependência tecnológica, a maior intensidade na concorrência e a globalização dos mercados, todos estes factores têm vindo a deixar as empresas mundiais mais expostas do que nunca ao risco operacional. Numa referência particular à indústria financeira, Buchelt e Unteregger (2004) argumentam que o risco de fraude e os eventos externos sempre estiveram presentes ao longo da história, mas foi o progresso da tecnologia que elevou o potencial do risco operacional – os avanços tecnológicos fomentam a rápida inovação financeira e a proliferação de produtos financeiros fortemente dependentes de serviços e sistemas bastante expostos a risco operacional, como é o caso do *e-banking*.

As instituições financeiras têm vindo a tomar consciência de que o risco operacional está presente em toda a sua actividade e de que a gestão deste risco deve ser abordada com o mesmo nível de importância que é dado ao risco de crédito ou ao risco de

mercado. Este aumento do interesse pela gestão de risco operacional tem sido estimulado por factores como (i) o crescente número e complexidade dos produtos financeiros hoje colocados no mercado e transaccionados à escala global, pelo que os próprios mecanismos de transacção, ao trazerem uma maior sofisticação e automatização, criam, outrossim, novas fontes de risco operacional; (ii) a introdução de mais requisitos por parte das entidades reguladoras, que vieram exigir um tratamento específico para o risco operacional, envolvendo novos métodos de cálculo, gestão e reporte; (iii) a conclusão, por parte da gestão de topo das instituições financeiras, de que os sistemas que têm suportado os processos de gestão do risco operacional são, em muitos casos, inadequados e de que uma gestão eficiente de risco operacional requer melhorias significativas em matéria de processos e tecnologias e (iv) o aumento do conhecimento acerca de aplicações práticas de técnicas estatísticas para a gestão de risco operacional, permitindo às instituições financeiras a aplicação destas técnicas aos seus programas internos de gestão deste risco.

A história dos sistemas de informação para a gestão de risco está intimamente ligada à evolução da própria gestão de risco como processo e disciplina (Levine 2007). Os sistemas de gestão de risco começaram por se desenvolver em torno da actividade seguradora para suportar modelos estatísticos que, com base em dados históricos de perdas, mortalidade e outros, eram utilizados para prever futuros sinistros e volume de prémios. Nas instituições bancárias, o foco prioritário foi direccionado para sistemas que suportassem as suas actividades de concessão de crédito através da avaliação do risco associado a cada operação e do acompanhamento da evolução desse risco ao longo do ciclo de vida dos contratos. A gestão do risco de liquidez também era alvo de reporte simples que pretendia associar activos e passivos por maturidade ou taxa. O desenvolvimento de novas metodologias, como o *Stress Testing*, e de modelos para a

gestão de risco, como o *Value-at-Risk* (VaR), levou a que, desde os anos 90, muitas instituições financeiras tenham começado a implementar sistemas de informação para endereçar estas novas questões e para capacitar os seus sistemas de *Front Office* com funcionalidades como a simulação de Monte Carlo ou a gestão de limites.

Também entre os supervisores tem vindo a aumentar o interesse pelas metodologias através das quais as instituições gerem o seu risco e sustentam as suas análises e decisões. Este envolvimento, consubstanciado nos Acordos Basileia II e Solvência II, tem enfatizado aspectos claramente associados aos sistemas de informação – tais como os dados existentes (a sua disponibilidade e qualidade), a modelação aplicada, o reporte disponibilizado à gestão interna e ao mercado – e o processo aglutinador de todas estas actividades.

Como já se referiu, o risco operacional foi o que recebeu um desenvolvimento mais tardio e, consequentemente, a implementação de sistemas de informação para a sua gestão é também a mais recente. Em todo o caso, o valor dos sistemas de informação para as organizações e para a gestão de risco operacional foi apresentando por Chorafas (2001) como um elemento-chave para a sua competitividade, apontando a identificação de fontes de risco operacional, juntamente com a melhoria da capacidade de marketing e impacto nas vendas, bem como a eficácia na gestão, como os três vectores principais da contribuição dos sistemas de informação para o processo de criação de valor nas organizações: dependendo do seu nível de sofisticação e da forma como é implementada, a tecnologia pode ajudar no controlo e na gestão do risco operacional. Chorafas (2001) afirma, contudo, que, para tal se tornar realidade, computadores, sistemas de comunicação e aplicações de software necessitam ser eficazmente melhorados.

Foi só após a publicação e implementação do Acordo Basileia II que, na sua maioria, as diversas instituições, consultoras e empresas de desenvolvimento de software começaram a investir esforços na construção de sistemas para a gestão de risco operacional. Presentemente, a sofisticação e a adequação destes sistemas às reais necessidades das instituições permanece, por isso, aquém dos actuais desafios colocados pelos mercados financeiros. É de esperar – não só com base na investigação académica efectuada, mas também na colaboração existente entre consultoras, empresas de software, instituições financeiras e supervisores – que, em breve, se assista a uma evolução significativa dos sistemas de suporte à gestão de risco operacional.

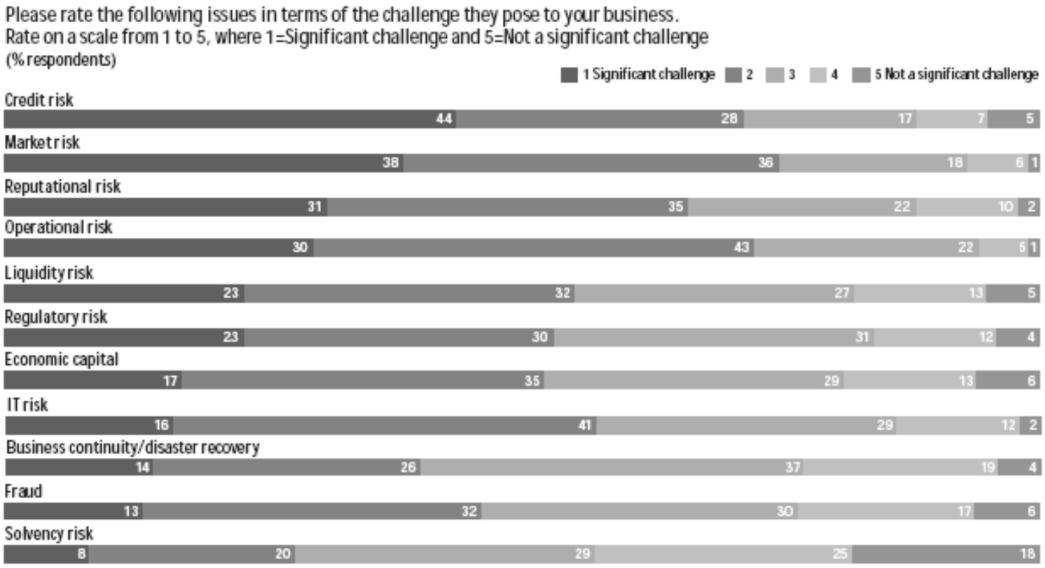
Apesar de o risco operacional ter sempre representado um dos riscos base da actividade financeira, a sua importância na gestão das instituições financeiras tem vindo a aumentar devido à emergência de novas ameaças à estabilidade financeira, como as geopolíticas, a fraca governação cooperativa e as vulnerabilidades sistémicas a um conjunto de derivados financeiros (Jobst 2007). A crescente sofisticação dos produtos financeiros, a diversidade de instituições financeiras e a progressiva interligação entre sistemas financeiros geram um efeito de globalização que aumenta o potencial para tornar mercados e ciclos de negócio altamente correlacionados, criando um meio para a propagação de riscos operacionais que podem pôr em causa a sustentabilidade do sector financeiro internacional. Torna-se, assim, indispensável que as instituições financeiras abordem a gestão de risco operacional como um factor crítico de sucesso, tão relevante como a gestão de risco de crédito ou de mercado, ou os seus processos de aquisição de clientes ou de investimento. Cabe aos sistemas de informação capacitar os órgãos de gestão das instituições com o conhecimento que lhes faculte tomar as decisões mais acertadas para evitar perdas, enfrentar ameaças e retirar valor de novas oportunidades.

1.1 – Relevância do tema

A gestão de risco operacional está já identificada como uma fonte de sucesso na actividade de uma instituição financeira; com o objectivo de o gerir, têm vindo a ser implementados sistemas de informação capazes de munir os gestores de ferramentas que lhes permitam aferir, de um lado, como os diferentes riscos afectam a sua empresa e, de outro, como estes são tratados pelas medidas de controlo que vão sendo implementadas.

Um estudo envolvendo 316 executivos de todo o mundo, efectuado durante o mês de Julho de 2008, que incluiu companhias de diferente dimensão da indústria financeira, demonstrou a relevância reconhecida tanto aos desafios como aos investimentos realizados e a realizar nas diversas áreas de risco. Como se pode observar na Figura 1 – Importância dos desafios colocados à organização –, se agregarmos os dois valores de elevada significância (1 e 2), o risco operacional encontra-se classificado entre os dois riscos que apresentam maiores desafios para a gestão. A falta de conhecimento sustentado sobre as formas de medir e gerir este risco, a sua transversalidade a todos os processos e linhas de negócio das instituições e as dificuldades resultantes da necessidade da sua identificação e reporte perfazem os principais factores desafiantes para a gestão de risco operacional.

Figura 1 – Importância dos desafios colocados à organização (Fonte: Enterprise risk management in financial service organizations – Economist Intelligence Unit)



A figura 2 – Investimentos nas áreas de risco – mostra que o risco operacional tem correspondido, no último ano, a uma das principais áreas de investimento; apresenta, inclusive, números que sugerem que a sua importância irá aumentar dentro das organizações, o que se reflecte nos investimentos que irão ser realizados. Estes resultados podem ser explicados através de duas vertentes: a primeira refere-se a ser este o risco em que o desenvolvimento está mais atrasado, logo, o que vai necessitar de mais investimentos para tornar a sua gestão efectiva; a segunda vertente que pode ser identificada é a extensão da gestão de risco operacional e dos seus sistemas de informação a áreas como o *Compliance* ou a Auditoria Interna – esta tendência tem-se acentuado porque existem várias sinergias entre estas três áreas que importa capitalizar dentro das instituições, tais como a partilha de catálogos de riscos e controlos, normas e regulamentação, medidas de mitigação, entre outras. É lícito afirmar que a não

integração destas três áreas num contexto corporativo cria inconsistência nos dados e nas análises utilizadas, o que irá fomentar factores de desarticulação interna nas instituições com implicações diversas nos processos de tomada de decisão, tais como os que se referem à opção de desenvolvimento de novos mercados ou à implementação de planos de continuidade de negócio.

Figura 2 – Investimentos nas áreas de risco (Fonte: Enterprise risk management in financial service organizations – Economist Intelligence Unit)

A necessidade de colocar esforços na gestão de risco operacional por parte das instituições financeiras é também reforçada através de estudos realizados nos Estados Unidos da América, conduzidos por Cummins et al. (2006) e Wei (2006), a propósito de eventos de risco operacional de elevado impacto. Nestes estudos, é demonstrado que um banco, ou outro tipo de instituição financeira, pode sofrer quebras no seu valor de mercado nos dias seguintes ao anúncio referente a uma perda elevada; quebras que poderão revelar-se superiores à própria perda inicial. Já Ong (2002) inventaria as dez principais razões que têm despertado o interesse pelo risco operacional, entre as quais, destaco as três primeiras: (i) carácter de novidade e de difícil compreensão; (ii) a

circunstância de as instituições financeiras acreditarem ter já conquistado tanto o risco de mercado como o de crédito e (iii) a possibilidade de o risco operacional equivaler a uma conveniente explicação para todos os tipos possíveis de riscos.

A elevada atenção depositada, por parte dos reguladores, no risco operacional pode ser atribuída à mudança no perfil desse risco no sector de serviços financeiros, resultante de factores como o crescimento do comércio electrónico, a crescente dependência tecnológica deste sector, o desenvolvimento de novos produtos e serviços de elevada complexidade e o emergente carácter global dos mercados. Todavia, foram alguns dos eventos de risco operacional já mencionados que puseram em causa a firmeza do sistema financeiro, motivando os reguladores para reforçar fortemente a supervisão sobre o risco operacional – o Comité de Basileia de Supervisão Bancária expressou, em 1999, a sua visão de que o risco operacional é "suficientemente importante para os bancos lhe dedicarem os recursos suficientes à sua quantificação".

Também as empresas de *rating*, como a *Moody's Investor Service (*Moody's Analytical Framework for Operational Risk Management of Banks, 2003) e a *Fitch Ratings* (Operational Risk Management & Basel II implementation: Survey Results, 2004), publicaram entre 2003 e 2004 relatórios acerca do papel da gestão de risco operacional nas empresas de serviços financeiros e do risco operacional no cálculo de *ratings* corporativos. Estes relatórios indicavam linhas orientadoras do que seria necessário, ao nível da sua governação e dos sistemas de informação, para que uma instituição financeira pudesse ser bem avaliada na vertente de gestão de risco operacional, tais como, a capacidade de avaliação de riscos e controlos.

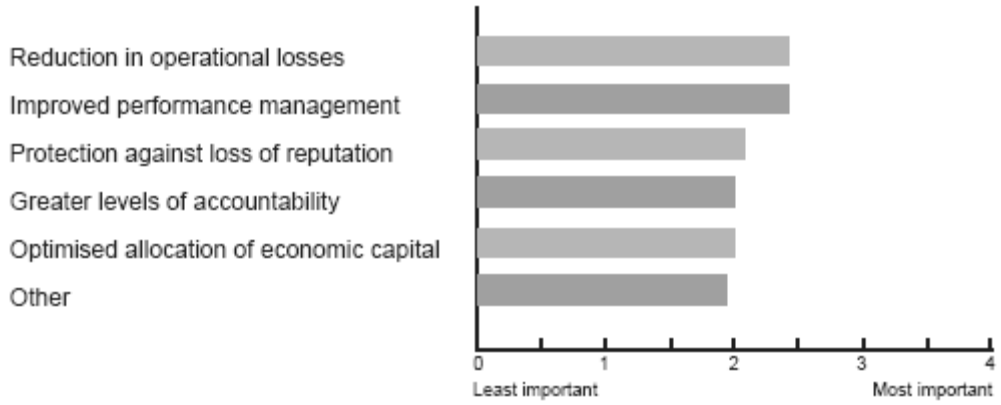
Se a resposta ao supervisor foi, em muitos casos, o principal argumento que conduziu ao desenvolvimento de gestão de risco operacional nas instituições financeiras, também existem razões internas para que esta gestão ganhe uma

importância crescente (Figura 3 – Importância da gestão de risco operacional), das quais se destacam a redução de perdas operacionais e a melhoria da performance. Sejam as razões de ordem interna ou externa, os resultados dos diversos estudos e iniciativas, tanto a nível académico (Cummings et al. 2006), quanto empresarial (Enterprise risk management in Financial service organizations 2008), suportam de forma consistente a visão de que o risco operacional representa uma ameaça significativa ao valor de mercado de bancos e seguradoras (sendo o "preço" deste risco utilizado no cálculo de valores futuros da empresa por parte dos potenciais investidores), fornecendo um racional para que as empresas façam uma gestão dos seus riscos operacionais, mesmo que esses riscos propendam para ser não sistémicos. Apesar de Lewis e Lantsman (2005) descreverem o risco operacional como idiossincrático, uma vez que "o risco de perda tende a ser não correlacionado com as forças gerais do mercado" – ou seja, quando uma empresa é atingida por risco operacional este não se dissemina para outras empresas –, esta visão de idiossincrasia do risco operacional é pouco sustentável porque implica que, sempre que um banco incorre numa perda por um incumprimento num crédito, ou por flutuações de mercado, a sua capacidade para fazer face às suas obrigações com outros bancos é afectada; não será o caso quando um banco incorre em perdas resultantes de actividades não autorizadas ou fraude. Contudo, em certos tipos de riscos operacionais, como a fraude, existe uma clara tendência para uma situação de contágio em que a partilha ou não partilha de informação entre instituições pode reduzir, ou, pelo contrário, elevar o risco operacional a que cada instituição está exposta.

A reacção dos mercados de capitais a anúncios de eventos de risco operacional suporta, igualmente, a perspectiva de que a disciplina de mercado poderá servir como uma ferramenta poderosa para que os supervisores incentivem a gestão de risco

operacional, no sentido de garantirem a transparência e a sobrevivência das instituições que regulam e do sistema no seu todo.

Figura 3 – Importância da gestão de risco operacional (Fonte: International Benchmark Survey Conducted by SAS and Risk Magazine, Agosto de 2003)



A capacidade de gerir o risco operacional depende frequentemente da existência de um sistema de informação em torno do qual uma instituição financeira possa reconfigurar as suas operações. A informação que alimenta estes sistemas apresenta-se como um dos pilares essenciais, mas também um dos principais problemas que a implementação destes sistemas vai enfrentar. Também ao nível das técnicas de análise e da metodologia de reporte existem áreas que necessitam de ser mais exploradas, de forma a criar sistemas de informação capazes de contribuir para uma maior eficiência e sustentabilidade das instituições financeiras. É, no entanto, fundamental ressalvar que estes sistemas de informação podem evoluir rapidamente e ser usados quer de uma forma eficiente, quer com incorrecções – Chorafas (2001) assegura que a sua utilização requer disciplina e visão por parte da gestão, podendo um sistema obsoleto, ou mal implementado, transformar-se em mais uma fonte de risco operacional.

Tendo como referência o estado de parca maturação dos sistemas de gestão de risco operacional relativamente aos dos outros riscos (Figura 4 – Estado de maturação da investigação na área de risco), é justo preconizar que tanto a prática como a ciência continuam à procura de um método eficiente para medir, controlar e gerir o risco operacional em instituições financeiras (Saidenberg & Schuermann 2003). Quer a indústria financeira, quer os investigadores serão agora e no futuro confrontados com a necessidade de desenhar modelos e sistemas de informação que respondam à dinâmica e à complexidade, cada vez maiores, das diferentes actividades em que as instituições vão estar envolvidas (Brink 2002). Esta evolução dos sistemas de informação irá passar não só pela melhoria e automatização de muitas das tarefas dos actuais sistemas, mas também por aspectos como a integração com outras aplicações e a expansão das funcionalidades a novas áreas, tornando a gestão de risco operacional num vector fundamental na gestão diária das instituições, bem como nos seus processos de tomada de decisão.

Figura 4 – Estado de maturação da investigação na área de risco (Fonte: Raft survey: Emerging Trends in Operational Risk 2002)

1.2 – Objectivo da tese

Este trabalho tem como objectivo cimeiro analisar o estado actual do desenvolvimento da implementação de sistemas de informação para gestão de risco operacional nas instituições financeiras em Portugal. Partindo da relevância dada por estas instituições, bem como pelas entidades reguladoras (de acordo com os documentos Basileia II e Solvência II), procurar-se-á identificar quais as necessidades, dificuldades e objectivos da implementação de soluções para a gestão de risco operacional; obter um claro entendimento da importância e do reconhecimento que é conferido ao risco operacional por parte das instituições financeiras em Portugal, e perceber o nível de envolvimento que estas instituições pensam dedicar à implementação de sistemas, mais ou menos sofisticados, para a gestão de risco operacional.

O segundo objectivo deste trabalho é o desenho conceptual de um sistema de informação que permita uma mais eficiente e eficaz gestão de risco operacional por parte das instituições financeiras. Este propósito deverá ser alcançado por meio da identificação das dificuldades dos actuais sistemas e dos requisitos apresentados pelas instituições financeiras, assim como através do recurso à recente investigação de que tem sido alvo o risco operacional. Este desenho conceptual de um sistema de informação para a gestão de risco operacional apresenta como finalidade atingir as seguintes metas: (i) responder aos requisitos impostos pelas entidades reguladoras no que concerne o cálculo e a gestão de risco operacional; (ii) apoiar as instituições na detecção de ameaças operacionais que possam pôr em questão os seus objectivos estratégicos ou mesmo a sua sobrevivência; (iii) capacitar as instituições com informação que lhes permita evoluir com sucesso em mercados cada vez mais complexos e dinâmicos.

II PARTE – CONCEITOS BASE

2 – RISCO OPERACIONAL EM INSTITUIÇÕES FINANCEIRAS

O papel da gestão de risco nas instituições financeiras evoluiu muito para além da simples mitigação dos riscos identificados, caminhando para uma disciplina que concentra modelos financeiros e econométricos complexos. Buchelt e Unteregger (2004) argumentam que, muito antes do advento do Acordo Basileia II, as instituições financeiras já tinham posto em prática vários mecanismos e procedimentos de controlo, defendendo que a gestão de risco operacional é mais antiga do que a gestão de risco de crédito ao mercado. No entanto, continua a ser uma realidade que a gestão de risco operacional tem sido um conjunto de actividades fragmentadas, desenhadas para lidar com uma vasta variedade de riscos operacionais. Uma vez que o conceito de risco operacional era desconhecido até há aproximadamente dez anos atrás – o termo "risco operacional" recebeu o reconhecimento geral em 1995, após a famosa falência do banco Barings –, não se afigura surpreendente que a gestão de risco operacional não perfaça ainda um processo integrado como o é no caso do risco de crédito ou de mercado.

Um estudo patrocinado pela Associação de Bancos Ingleses mostrou que os bancos seus associados estimam a divisão dos principais riscos da seguinte forma (Cruz 2003):

1. Crédito – 60%
2. Mercado / liquidez – 15%
3. Operacional – 25%

Estes números aparentam ser estimativas relativamente duvidosas, sendo expectável que presentemente nenhum banco tenha uma medida fiável das suas perdas relativamente a risco operacional (existem bancos que já têm implementados mecanismos de recolha de dados mas com uma cobertura ainda parcial dos seus

processos de negócio). No caso específico das instituições seguradoras, poucas estão a tentar quantificar o risco operacional e incorporá-lo em modelos avançados. O risco operacional encontra-se normalmente presente e até se correlaciona com outras áreas de risco – muitas das falhas na indústria seguradora que foram atribuídas ao risco operacional correspondem, na verdade, a uma combinação de lacunas de processos e de gestão. Estes factores, juntamente com a inadequação dos recursos financeiros, revestem-se de primordial importância para garantir a protecção de uma seguradora contra a insolvência.

2.1 – Definição de risco operacional

Há muito pouco acordo entre académicos e profissionais sobre o conceito de risco operacional, assim como as suas causas, consequências, características e gestão. Ao passo que existe consenso na visão de que o risco operacional é diverso e de difícil quantificação, predomina um desacordo considerável quanto à definição de risco operacional, à sua classificação e sobre o que deve ou não ser incluído neste conceito.

Crouchy (2001) sugere que o risco operacional integra um conceito difuso devido à complexidade em fazer a sua clara distinção perante as incertezas habituais que todas as organizações precisam de enfrentar nas suas actividades diárias. Já Rao e Dev (2006) argumentam que há sete anos não era incomum considerar o risco operacional como algo residual, uma categoria de risco para a qual concorria tudo o que não fosse passível de considerar como risco de crédito ou de mercado.

Em 1993, o Grupo dos 30 (um grupo consultivo internacional para assuntos económicos e financeiros, composto por elementos dos sectores público e privado e da Academia) descreveu risco operacional como a “incerteza relacionada com perdas

resultantes de sistemas ou controlos inadequados, erros humanos ou gestão". O Banco da Austrália avançou, em 1999, com uma explicação mais abrangente de risco operacional, a saber, "todos os riscos que não sejam risco de crédito ou mercado, que possam causar volatilidades nos proveitos, despesas e no valor de negócio dos bancos". Numa definição apresentada no ano anterior no Banco da Reserva Federal de Nova Iorque, Shepheard-Walwyn e Litterman (1998) caracterizaram o risco operacional como "um termo geral que se aplica a todas as falhas que influenciem a volatilidade da estrutura de custos da empresa ou estrutura de proveitos". Finalmente, nesse mesmo ano, uma definição que identificava fontes internas e externas de risco operacional foi avançada por Crouchy et al. (1998), que propuseram que por risco operacional se entende "o risco de eventos externos, ou deficiências em controlos internos ou sistemas de informação, [que] resultem numa perda, quer esta seja antecipada ou completamente inesperada". Já Lopez (2002) advogou que risco operacional coincide com "todo o tipo de risco não quantificável que um banco possa enfrentar".

A mais usual das definições de risco operacional foi apresentada, pela primeira vez, por Morris et al. (1999), que o interpretaram como "a perda directa ou indirecta resultante de processos internos inadequados, falhas, pessoas, sistemas, ou de eventos externos". Inicialmente, o Comité de Basileia adoptou esta definição, mas a referência a perdas indirectas foi subsequentemente eliminada devido ao pressuposto da quantificação de capital regulamentar, já que estas perdas apresentam obstáculos à sua medição. Assim, o Acordo de Basileia II definiu risco operacional como "o risco resultante de processos internos inadequados, falhas, pessoas, sistemas, ou de eventos externos". Esta definição, que se baseia nas causas subjacentes (fontes) de risco operacional, inclui o risco legal, mas exclui os riscos de negócio e reputação.

Desde o início, surgiram várias críticas a esta definição. Herring (2002) critica-a com base na simples exclusão do risco de negócio no seu todo. Thirlwell (2002) argumenta que a definição do Comité de Basileia representa uma "visão mensurável de risco operacional para quem está a tentar avançar com algo que seja quantificável, mas inadequada para identificar as causas que levam os bancos a falharem".

Em 2005, Vinella e Jin avançaram com uma nova descrição de risco operacional, nomeadamente "o risco de a operação vir a falhar um, ou mais objectivos de performance operacional, quer esta seja pessoas, tecnologia, processos, informação, ou a infra-estrutura que suporta as actividades de negócio".

Na presente investigação e nas propostas apresentadas, é utilizada como base a definição dada por Vinella e Jin (2005), por representar uma visão mais global do que deve ser a gestão de risco operacional nas instituições financeiras, essencialmente devido a se concentrar nos objectivos da instituição e não apenas nas perdas derivadas de riscos operacionais. Esta enunciação engloba os objectivos fundamentais que devem estar presentes na gestão de risco operacional, assim como nos sistemas de informação que a suportam – visão integrada de todas as fontes possíveis de risco operacional, bem como das diferentes dimensões que encapsulam a actividade de uma instituição (processos, informação e os diversos agentes intervenientes nas diferentes actividades) – , e os objectivos que podem passar não só pela redução de perdas, como também pela identificação de oportunidades de melhoria ou da procura de novas opções estratégicas. Para efeitos das entrevistas efectuadas, foi considerada, porém, a definição apresentada no Acordo Basileia II, pois esta é a que apresenta uma utilização mais difundida na maioria dos bancos, seguradores e entidades supervisoras, na qual, numa primeira fase, estas instituições basearam as suas metodologias e desenvolvimentos. O emprego das duas definições não coloca qualquer tipo de problema ao processo de investigação, pois

a definição apresentada por Basileia II representa um subconjunto do conceito mais global da proposta de definição apresentada por Vinella e Jin, englobando, esta última, objectivos mais abrangentes para a gestão de risco operacional.

2.2 – Gestão de risco operacional

Analisando todas as definições e tipos de risco operacional, somos persuadidos a concordar que a sua característica principal é a diversidade. Esta diversidade torna difícil limitar o número de dimensões de análise e metodologias de gestão. Qualquer que seja a metodologia utilizada para a gestão de risco operacional, existem três dimensões fundamentais que caracterizam qualquer fenómeno de risco operacional: a causa ou fonte (os factores de risco que provocam, ou podem potenciar, a ocorrência de determinado evento), o tipo de risco (as características do risco associado ao evento) e a consequência (os impactos resultantes para a instituição da ocorrência do evento).

Segundo Wahler (2002), enquanto os eventos de risco de mercado ou de crédito são influenciados por transacções e parceiros de negócio da instituição, o risco operacional deriva de três fontes genéricas internas e externas, a saber, (i) mudança: causas externas e internas que influenciam a estratégia da instituição; (ii) complexidade: em produtos, processos e tecnologia; (iii) complacência: gestão ineficiente do negócio e do seu risco.

Diferentes categorias de risco foram já apresentadas para classificar eventos de risco operacional, das quais se têm destacado a apresentada pelo Comité de Basileia II para a banca e a proposta pelo COBIT (*Control Objectives for Information and Related Technology*) para a área das tecnologias de informação. É, no entanto, de realçar que, na sua maioria, as instituições financeiras têm desenvolvido os seus próprios catálogos de

riscos para classificação dos seus eventos, mesmo que tal exija mapear os seus tipos de riscos para os catálogos de riscos do supervisor.

A terceira dimensão é a consequência, ou seja, o impacto financeiro, ou não financeiro, que a instituição pode ter de enfrentar. Kingsley et al. (1998) identificaram três tipos de impacto que podem resultar de eventos de risco operacional: (i) perdas financeiras directas como, por exemplo, perdas relativas a fraude ou a coimas; (ii) perdas financeiras indirectas, tais como perdas relativas a má reputação ou à necessidade de alocação de mais recursos a certas actividades e (iii) redução de proveitos devido à falta de operacionalidade de fazer negócio, do qual constituem exemplos as perdas de receita por causa da incapacidade da instituição em responder aos requisitos dos clientes.

Na análise da dimensão "consequência", emerge um determinante fundamental que é necessário estudar – a mitigação. A existência ou não de mecanismos de mitigação desempenha uma influência significativa sobre o real impacto para a instituição de um determinado risco. Kaiser e Kohne (2006) argumentam que a característica mais endógena do risco operacional em relação aos riscos de mercado ou crédito significa que as oportunidades de mitigação de risco são frequentemente maiores no caso do risco operacional. A utilização das medidas de mitigação para redução de impactos, sem esquecer os custos associados à sua implementação ou manutenção, deverão ser consideradas no cálculo da taxa de retorno da instituição.

O Comité de Basileia (2001), ao definir a gestão do risco financeiro como uma sequência de quatro processos – ou seja, a classificação dos eventos em uma ou mais subcategorias de risco de mercado, crédito, operacional ou "outros" riscos; a compreensão desses riscos utilizando dados e modelos; a apresentação regular de relatórios e o controlo desses riscos pela gestão de topo (Alexander 2004) –, vem

orientar claramente os objectivos da gestão de risco operacional para a identificação e a medição dos riscos operacionais que podem pôr em causa a sobrevivência das instituições com base nas três principais dimensões já identificadas – fonte, risco e consequência. Em todo o caso, autores como Kingsley et al. (1998) identificam objectivos mais abrangentes para a gestão de risco operacional: (i) evitar perdas catastróficas; (ii) gerar uma compreensão abrangente dos temas de risco operacional; (iii) capacitar a empresa para antecipar o risco de forma efectiva; (iv) fornecer uma medida de performance objectiva; (v) mudar comportamentos para reduzir o risco operacional; (vi) fornecer informação objectiva para que os serviços oferecidos pela empresa tenham em conta o risco operacional e (vii) assegurar que são tomadas as precauções correctas aquando de fusões e aquisições.

Diferentes metodologias concorrem para a concretização destes objectivos, de entre as quais, são apresentadas, neste trabalho, duas das mais aplicadas na indústria financeira. Ambas centram a sua análise na dimensão "processos de negócio" das instituições financeiras, visão algo diferente da apresentada pelo Acordo Basileia II, que centra as suas análises nas dimensões linha de negócio e categoria de risco. Kross (2009) apresenta fundamentos para esta abordagem por processos e dirige uma crítica rigorosa a esta classificação matricial aplicada por Basileia II, afirmando que este Acordo ignora alguns aspectos reais encontrados nas instituições financeiras, tais como a interdependência de processos ou o impacto transversal de normas e regulamentação. Na sua maioria, as instituições financeiras portuguesas centraram, também, os seus programas de risco operacional numa abordagem por processos.

A primeira abordagem é apresentada por Marshall (2001), que a define como um procedimento de análise sistemática dos processos e recursos críticos e dos eventos e factores de risco que podem afectar esses processos e recursos. A gestão de risco

operacional deve ser sistemática na análise das causas subjacentes às perdas esperadas e não esperadas, assim como na avaliação do racional para a prevenção de risco, mitigação, transferência e financiamento. Este processo é composto por seis etapas: (i) definição de âmbito e objectivos – esta etapa deve estabelecer qual o factor determinante para a existência de um processo de gestão de risco operacional, seja este por pressões regulamentares ou por razões internas como a redução de perdas; também, nesta etapa, devem ser estabelecidos os objectivos para o processo, como sejam a melhoria da eficácia operacional ou a avaliação de riscos e controlos; deve ser criada, outrossim, uma estrutura de governação para a gestão de risco operacional e estabelecidas as políticas internas de comunicação, motivação e recompensa associadas à gestão de risco operacional; (ii) identificação dos riscos críticos – nesta etapa, devem ser identificados processos, recursos e eventos críticos, sendo que os critérios para esta selecção devem estar directamente alinhados com os objectivos estabelecidos na etapa anterior; (iii) estimação de riscos – através do recurso a dados de diferentes fontes (informação histórica, questionários e indicadores de risco), devem ser construídas estimativas para os principais factores de risco operacional associados aos processos e recursos identificados na etapa precedente; nesta fase, a gestão deve definir os critérios de magnitude em relação ao impacto de cada tipo de risco na instituição financeira, da probabilidade de eventos ocorrerem, bem como da interdependência entre riscos; (iv) análise de riscos – nesta etapa, o efeito agregado das perdas deve ser estimado, isto é, devem ser avaliadas medidas alternativas de gestão e análise dos eventos e factores de risco operacional, quer numa base individual, quer numa base corporativa; (v) implementação de acções de gestão – esta etapa cobre um conjunto vasto de actividades para a gestão dos riscos existentes nos processos e recursos identificados; estas actividades englobam a decisão de aceitar ou evitar certos riscos, a previsão de perdas

futuras, a redução do impacto dos riscos em determinados processos ou o recurso a medidas de financiamento (e.g. seguros); (vi) controlo e reporte – os processos, os recursos e os riscos a eles associados devem ser alvo de um contínuo controlo e reporte, para que o processo de gestão de risco operacional possa acompanhar as mudanças que vão ocorrendo nas actividades das instituições, tais como o desenvolvimento de novos produtos e mercados. Para que todas estas etapas se congreguem rumo ao estabelecimento de um processo de gestão de risco operacional de sucesso, deverão ser estendidas à organização no seu todo e não ficar cingidas à função de gestão de risco.

Dickstein e Flast (2009) apresentam a sua metodologia, baseada na arquitectura BPM (*Business Process Management*), como um ciclo, reflectindo a natureza recorrente da gestão de um processo. Este ciclo é composto por quatro etapas que se interligam com o processo de BPM das instituições – tal como já foi salientado, os processos são a principal dimensão que está a ser adoptada pelas diferentes instituições na sua gestão de risco operacional. A primeira das quatro etapas pretende alinhar os objectivos de negócio com os limites ao risco da instituição, na qual a tolerância a riscos operacionais deve ser incluída nas opções estratégicas – deve ser também estabelecida uma arquitectura de gestão de risco que as suporte. Na segunda etapa, são identificados os riscos potenciais associados aos diferentes processos – por outras palavras, são reconhecidos, para cada processo, as potenciais ameaças e deficiências, bem como os pontos de controlo implementados para a sua mitigação. Esta fase implica um trabalho detalhado sobre o funcionamento da instituição, além de que requer um elevado nível de racionalidade para evitar situações nas quais são negligenciados riscos elevados, ou situações de excesso de zelo, onde até o menor desvio ao que está no desenho do processo é considerado risco operacional – deverá existir sempre um nível de tolerância (definido na etapa anterior), abaixo do qual as situações de risco operacional são

ignoradas. A terceira etapa serve para controlar os processos e o seu risco. Somente através da recolha contínua de informação sobre os processos e os riscos é que a gestão de risco operacional pode ser embebida no processo diário de gestão. A recolha de dados como os KRI's (*Key Risk Indicators*) torna-se útil para garantir que processos e riscos estão de acordo com o que foi delineado na primeira etapa e que a instituição continua a executar a estratégia planeada, dentro dos limites que foram estabelecidos. A última etapa cobre a gestão activa de processos e risco; é precisamente neste ponto que a instituição deve estabelecer as acções de mitigação para risco operacional – deve estudar, para isso, todos os diferentes cenários, que podem ir desde o reforço das medidas de controlo existentes até ao próprio redesenho de todo o processo. A grande força desta metodologia reside na sua clara interligação com a gestão do processo da instituição e na possibilidade de criar um elevado alinhamento entre os objectivos da instituição, os seus processos desenhados para os concretizar e a gestão dos riscos e controlos associados aos processos, que podem comprometer o alcance dos objectivos.

Já no ano de 2010, o Instituto de Actuários do Canadá publicou o documento "Uma Nova Abordagem para a Gestão de Risco Operacional" (Society of Actuaries 2010), no qual apresenta uma nova abordagem *top-down*, que se concentra, numa primeira fase, nos riscos mais consideráveis das instituições, só descendo para níveis de maiores granularidades nas áreas onde essa necessidade for identificada. Este documento defende que esta abordagem permite às instituições melhorarem o foco do seu processo de gestão de risco, necessitando de menos recursos humanos e financeiros, pois evita que a gestão se debruce sobre riscos imateriais para a instituição. As diferenças mais significativas desta abordagem no processo de gestão de risco em relação a abordagens mais tradicionais podem ser sintetizadas em três vectores principais: em primeiro lugar, (i) a definição de risco. Enquanto, nas abordagens mais tradicionais, risco é descrito

como um tipo de evento não desejado (e.g. fraude, falha de sistemas), na abordagem apresentada neste documento, risco é definido como uma medida da exposição a uma perda em resultado de um evento. Em segundo, está (ii) o processo de identificação de riscos. Nas abordagens tradicionais, é pedido aos gestores das unidades de negócio que identifiquem os seus maiores riscos, o que, no final, implica que a instituição fique com um conjunto vasto e de difícil gestão. No documento dos actuários canadianos, este processo começa pela identificação de um conjunto finito de classes de risco por parte da instituição, recorrendo-se, depois, à utilização de dados quantitativos e qualitativos para o escrutínio das áreas nas quais as perdas mais elevadas estão a ocorrer. Finalmente, (iii) existem diferenças quanto aos objectivos de cada uma destas abordagens. Ao passo que, na visão mais tradicional, o objectivo equivale à gestão diária das ameaças que surgem de eventos operacionais, na abordagem apresentada pelos supramencionados actuários, os objectivos correspondem à gestão dos riscos-chave e à optimização dos controlos associados a estes riscos, sempre num contexto de análise custo benefício.

Qualquer que seja a metodologia adoptada pelas instituições financeiras, ela deve ser objectiva na concretização das metas que lhe foram atribuídas pelos órgãos de gestão, assim como apta a responder àqueles que são os requisitos definidos por cada um dos supervisores para a gestão de risco operacional.

Um aspecto fundamental na gestão de risco operacional coincide com o papel da função de gestão de risco. O objectivo primário desta função assenta em facilitar, de forma efectiva, a gestão de risco, que deverá ser da responsabilidade das unidades de negócio ou da gestão de topo da instituição. Para garantir este objectivo, cabe ao órgão de gestão de risco operacional desenvolver na instituição uma cultura de risco que harmonize os objectivos de decisores, accionistas e supervisores. Aquele deverá

disponibilizar, outrossim, uma arquitectura, uma infra-estrutura, ferramentas e metodologia para permitir à gestão incorporar a gestão de risco operacional no seu processo global de gestão de riscos, em conformidade com análises custo-benefício e dentro dos limites de tolerância ao risco definidos na instituição. Por fim, deve assegurar a transparência nos processos de análise e gestão de risco operacional, para que entidades independentes possam avaliar a exactidão e o valor da informação disponibilizada e das medidas de mitigação implementadas. O Instituto de Actuários do Canadá, no mencionado documento (Society of Actuaries, 2010), declara que a responsabilidade da função de gestão de risco operacional deverá ser a de fornecer à gestão, dados, ferramentas e técnicas que lhe permita: (i) determinar a magnitude da exposição a cada um dos maiores riscos e respectivos mecanismos de controlo, para permitir verificar se os níveis de tolerância ao risco estão a ser cumpridos; (ii) no caso de riscos mais significativos, avaliar, numa análise custo-benefício, a possibilidade de implementação de medidas de mitigação; (iii) para novas oportunidades de negócio, determinar qual o impacto de novos projectos nos níveis de risco operacional da instituição, analisando, especialmente, se os ganhos previstos irão compensar o incremento no risco operacional.

Em muitas instituições, o papel da gestão de risco operacional nunca esteve bem definido. Na falta de objectivos tangíveis, esta área acolhia um conjunto de actividades estanques, desenhadas para responder a supervisores, empresas de *rating* e requisitos de auditoria. A nova regulamentação (e.g. Basileia II, Solvência II, SOX) veio ajudar a criar um espaço próprio para a gestão de risco operacional nas instituições financeiras através de criação de novas estruturas orgânicas, ou do desenvolvimento, em estruturas existentes, de novas funções dedicadas a este risco. Apesar dos fortes investimentos realizados, muitas instituições não estão impressionadas com os resultados obtidos pela

gestão de risco operacional, não só porque muitos dos procedimentos que são realizados por estas novas estruturas se assemelham muito aos que eram normalmente efectuados pela Auditoria Interna ou pelo *Compliance*, mas também por requererem um conjunto de actividades que exigem numerosos recursos das unidades de negócio, sem que pareçam produzir, contudo, outros benefícios para a instituição, para lá de esta poder afirmar que está de acordo com as normas do supervisor. No entanto, a existência de um programa corporativo de gestão de risco operacional pode proporcionar, a uma instituição, atingir objectivos que lhe faculte incrementar aspectos estratégicos da sua actividade ao (i) assistir os gestores executivos na gestão pro-activa do risco operacional; (ii) monitorizar o desempenho da instituição e avaliar periodicamente as suas linhas de negócio; (iii) suportar a análise de dados internos, determinar que lições podem ser apreendidas e desenvolver estratégias para minimizar e prevenir problemas futuros; (iv) quantificar risco operacional por linha de negócio e (v) demonstrar preocupações de risco operacional, em concerto com as leis e regulamentos aplicáveis. As instituições que atinjam estes objectivos poderão esperar um maior retorno do seu investimento através da redução das suas perdas e custos operacionais, do aumento das margens de lucros, da melhoria da eficiência dos seus processos e do reconhecimento da qualidade da sua gestão por parte do supervisor e do mercado em geral.

2.3 – Nova regulamentação para a gestão de risco operacional

Actualmente já existe um conjunto de regulamentação que "conduz" as instituições financeiras para uma melhor gestão do risco operacional. Muita desta regulamentação foi essencialmente produzida para proteger o sistema financeiro e os investidores de perturbações no sistema que pudessem, de alguma forma, colocar em risco, não só as

próprias instituições em que o risco surgisse, mas também todo o sistema no qual se encontram integradas. No âmbito deste trabalho, são apresentadas três destas estruturas regulamentares, a saber, o Acordo Basileia II para instituições bancárias, o Acordo Solvência II para a indústria seguradora e o decreto Sarbanes-Oxley, desenvolvido nos Estados Unidos da América, a cujos requisitos algumas empresas em Portugal decidiram responder.

2.3.1 – Acordo Basileia II

O risco operacional perfaz uma parte fundamental dos processos de negócio dos bancos e não pode ser completamente eliminado – é interesse comum de bancos e supervisores que este risco seja identificado, medido e controlado. Com esse objectivo, o Acordo Basileia II introduz o tratamento do risco operacional – os bancos irão ter de reter capital regulamentar para este risco (pilar I); observar os requisitos de gestão definidos pelas entidades supervisoras (pilar II) e apresentar relatórios relativos aos seus níveis de exposição, capital alocado e políticas de gestão de risco (pilar III) (Nash 2003) – estes três pilares também são aplicáveis ao risco de mercado e ao risco de crédito.

O Novo Acordo de Basileia II aborda, pela primeira vez, a questão do risco operacional, sendo o único tipo de risco a receber uma definição regulamentar oficial por parte do Comité de Basileia (o risco de mercado e o risco de crédito não têm definições oficiais), o que parece indicar o reconhecimento da complexidade, e porventura algum desconhecimento, dos conceitos e das metodologias associadas a este tema. Assim, Basileia II define o risco operacional como “o risco resultante de processos internos inadequados, de falhas, pessoas e sistemas, ou de eventos externos”. Esta definição inclui risco legal, mas exclui risco estratégico e de reputação. Este

Acordo também apresenta a definição de perda para efeitos de risco operacional como todo o custo com a resolução de um problema operacional, pagamento a terceiros, redução no valor dos activos, ou abate de activos.

Em relação ao cálculo de requisitos de capital requerido no pilar I do Acordo de Basileia, existem três abordagens à disposição das instituições bancárias (Basileia II 2003): (i) abordagem do indicador básico, que baseia o cálculo do capital numa percentagem fixa sobre um indicador da actividade do banco – neste momento, o volume de negócios; (ii) abordagem standard, que também se serve de um indicador da actividade bancária, como o volume de negócios, mas utiliza diferentes percentagens para distintas, e pré-definidas, linhas de negócio; (iii) abordagem de métodos avançados (AMA), sendo que o objectivo desta abordagem é fornecer uma arquitectura em que os bancos façam a sua auto-avaliação do seu risco operacional de uma forma mais avançada e rigorosa, alicerçada nos seus dados internos e em dados externos e que permita, outrossim, à entidade supervisora, a validação dos modelos utilizados. Na abordagem AMA, a instituição poderá reconhecer o impacto da mitigação nas medidas do risco operacional utilizadas para o cálculo dos requisitos de capital regulamentar – o reconhecimento da mitigação em seguros estará limitado a 20% do capital total de risco operacional, calculado segundo a abordagem AMA.

As instituições são encorajadas a avançar no espectro das abordagens disponíveis, à medida que desenvolvem práticas e sistemas de medição de risco operacional mais sofisticados. As instituições poderão usar a abordagem do Indicador Básico ou a abordagem Standard para algumas partes das suas operações e utilizar, simultaneamente, a abordagem de Medição Avançada para outras partes, desde que certos critérios mínimos definidos no Acordo sejam respeitados. Uma vez adoptada uma abordagem avançada de cálculo de requisitos de fundos próprios, a instituição não

poderá reverter para uma abordagem mais simples sem que essa alteração seja aprovada pelas autoridades de supervisão.

Existem diferentes críticas à estrutura deste pilar. McConnell (2008) questiona a relação entre perdas relativas a risco operacional e o volume de negócios, sustentando que não existe uma relação directa entre a dimensão de uma instituição e o nível de risco a que está exposta. Sundmacher (2007) demonstra que uma instituição pode ter muito poucos incentivos para investir na infra-estrutura necessária para a abordagem standard em relação ao indicador básico, devido aos custos desse investimento terem um impacto reduzido em termos de redução de alocação de capital. Quanto à abordagem AMA, Herring's (2002) argumenta que esta abordagem requer um conjunto de pré-condições a que a maioria das instituições só conseguirá responder após longos anos de implementação. Já Doerig (2003) defende que a gestão de risco operacional vai muito além da alocação de capital; é uma questão de boa gestão corporativa e, por isso, não deveria ser alocado capital para este risco, devendo os supervisores e os bancos concentrarem-se na implementação do seu processo de gestão de acordo com as disposições do pilar II.

O pilar II foi desenhado para assegurar que uma arquitectura de risco operacional foi desenvolvida na instituição e que o processo é adequadamente auditado e supervisionado. Tem por objectivo encorajar as instituições a tomar medidas preventivas da ocorrência de perdas operacionais, centrando-se em quatro princípios fundamentais (Basel II 2003): (i) os bancos devem ter mecanismos para identificar e calcular os seus riscos; (ii) as entidades supervisoras devem assegurar que os bancos fazem esta identificação e o cálculo de uma forma correcta e, no caso de tal não acontecer, que tomam as medidas correctivas adequadas; (iii) as entidades supervisoras devem assegurar que os bancos trabalham acima dos capitais mínimos regulamentares e

(iv) que actuam antecipadamente quando houver a possibilidade de este valor não ser atingido, impondo ao banco a reposição desses valores mínimos. Kaufman (2005) critica estes princípios por serem demasiado gerais e não levarem em conta as capacidades de auditabilidade de cada supervisor em diferentes países.

O pilar III tem como objectivo encorajar a disciplina de mercado através do desenvolvimento de um conjunto de informação que permite aos distintos participantes no mercado avaliar indicadores-chave sobre a gestão de risco operacional das instituições. O banco deve apresentar um conjunto de informações que inclui, entre outras, a estratégia para gestão de risco operacional, os métodos de mitigação, a abordagem utilizada para o cálculo do capital regulamentar e o valor desse mesmo capital. Uma das críticas mais comuns a este pilar assenta no facto de se afigurar muito pouco detalhado no que respeita a requisitos de disciplina de mercado, representando mais um conjunto de requisitos para reporte e transparência (Lopez 2003).

Como parte do pilar II do Acordo, o Comité de Basileia produziu o documento "*Sound Practices for the Management and Supervision of Operational Risk*", com um conjunto de práticas que os bancos deverão implementar de forma a gerirem melhor o seu risco operacional. Este documento inclui, por exemplo, a recomendação da criação de um ambiente de gestão de risco operacional (Currie 2004). De acordo com o mesmo documento, as instituições financeiras deverão adoptar um conjunto de medidas que visem o acompanhamento e controlo do risco operacional, de modo a poderem implementar as diferentes abordagens. Do conjunto de medidas apresentadas, o autor destaca as seguintes, como as mais significativas para o desenvolvimento de sistemas de informação para gestão de risco operacional (BCBS 2003):

1. A instituição deverá ter um sistema de gestão de risco operacional com claras responsabilidades associadas à função de gestão do risco operacional. Este

sistema tem de ser conceptualmente consistente e implementado com integridade;

2. A função de gestão de risco operacional será responsável por desenvolver estratégias para identificação, monitorização, controlo e mitigação do risco operacional; pela definição de políticas firmes e procedimentos relativos à gestão e controlo do risco operacional; pelo desenho e implementação do modelo de risco operacional da instituição e pelo desenho e implementação de um sistema de reporte de risco operacional;
3. A instituição deve localizar sistematicamente dados de risco operacional relevantes, incluindo perdas materiais por linha de negócio. O sistema interno de medição do risco operacional deve estar intimamente integrado com os processos de gestão de risco da instituição. Os seus outputs devem constituir parte integrante do processo de monitorização e controlo do perfil de risco operacional da instituição. Esta informação deve desempenhar um papel proeminente no reporte, na gestão e na análise de risco;
4. Há que existir um reporte regular da exposição da instituição a risco operacional e perdas associadas por unidades de gestão e linhas de negócio, gestores seniores e Conselho de Administração;
5. Deve existir documentação adequada do sistema de gestão do risco operacional, em termos de políticas internas, controlos e procedimentos;
6. Os processos de gestão de risco operacional da instituição e o sistema de avaliação devem ser sujeitos a validação e a uma revisão regular independente. Estas revisões têm de incluir tanto as actividades das linhas de negócio, como a função de gestão de risco operacional;

7. O sistema de avaliação de risco operacional da instituição (incluindo os processos de validação interna) deve ser sujeito a revisões regulares por parte de auditores externos e entidades supervisoras;
8. O sistema interno de medição de risco da instituição deverá estimar as perdas inesperadas, baseado numa combinação de dados relevantes de perdas externas e internas, análises de cenários, ambiente específico do negócio da instituição e factores de controlo internos;
9. O sistema de medição deverá ser capaz de calcular a alocação de capital económico para risco operacional ao longo das linhas de negócio, criando incentivos para a melhoria dos processos de gestão;
10. O sistema interno de medição do risco operacional deve estar intimamente integrado com os processos diários de gestão de risco da instituição. Os seus outputs devem constituir parte integrante do processo de monitorização e controlo do perfil de risco operacional;
11. A validação do sistema de gestão de risco operacional por auditores externos e pelas autoridades de supervisão deve incluir:
    a. A verificação de que os processos internos de validação estão a operar de forma satisfatória;
    b. A verificação de que os fluxos de dados e os processos associados ao sistema de medição de risco são transparentes e acessíveis.
12. Qualquer sistema de medição de risco operacional tem de ser consistente com a definição / âmbito de risco operacional e tipos de eventos de perda definidos pelo supervisor;
13. As entidades supervisoras irão exigir à instituição o cálculo de requisitos de capital regulamentar, como sendo a soma das perdas esperadas (*expected loss* –

EL) e das perdas inesperadas (*unexpected loss* – UL), a menos que a instituição demonstre que é mais adequado capturar as perdas esperadas nas suas práticas internas de negócio;

14. O sistema de medição de risco deve ser suficientemente granular para capturar os principais factores de risco operacional que afectam a distribuição da "cauda" das estimativas de perda;
15. Medidas de risco para diferentes estimativas de risco operacional devem ser adicionadas com o objectivo de cálculo dos requisitos mínimos de capital regulamentar;
16. Qualquer sistema de risco operacional tem que ter certas características-chave, ao encontro do conjunto de *standards* aconselhados pelas autoridades supervisoras. Esses elementos devem incluir o uso de dados internos relevantes, dados externos, análise de cenários e factores reflectindo o ambiente de negócio e sistemas de controlo interno.

A gestão de risco operacional, como a desenhada por Basileia II, foi criticada por Rebonato (2007) com base nas diferenças existentes entre reguladores e gestores de risco. Enquanto os reguladores estão preocupados com eventos catastróficos (representados pelo percentile 99.9 da distribuição de perdas), a gestão de risco está mais interessada no retorno diário das suas operações – o capital regulamentar foi desenhado para proteger os bancos de eventos catastróficos, ao passo que o capital económico é necessário para gerir o banco de forma eficiente. Currie (2006) alerta, por seu lado, para as dificuldades de implementação de métodos mais avançados por parte de bancos de mais pequena dimensão, o que fará com que estes fiquem em desvantagem competitiva em relação a bancos com recursos mais elevados. Pezier (2003) é crítico

perante o não reconhecimento dos riscos de negócio e de reputação por parte de Basileia II; defende, pois, que estes podem ser mais significativos do que as perdas operacionais directas – esta exclusão não se deveu a se ter reconhecido uma menor importância a este risco, mas sim à clara dificuldade em medi-lo e calcular o valor de capital a alocar.

Fundamentalmente, a questão fulcral não passa por saber se os bancos vão implementar os três pilares do Acordo, já que, na maioria das jurisdições, a sua implementação será imposta por legisladores e supervisores, mas sim se vão considerar a gestão de risco operacional como mais uma intrusão dos reguladores ou como uma oportunidade para observar e avaliar o seu negócio de uma maneira mais coerente (Nash 2003).

2.3.2 – Acordo Solvência II

Tipicamente, o risco operacional é uma área negligenciada no sector segurador, porque as instituições tendem a concentrar-se em áreas mais tradicionais de risco de seguro e riscos financeiros. De igual forma, historicamente as seguradoras têm disposto de muito poucos dados para sustentar as suas avaliações de risco operacional, tendo os seus modelos de capital se centrado em áreas onde existem mais dados para basear as suas análises, como o risco de seguro ou o risco de mercado. O Acordo de Solvência II acaba por provocar uma mudança nesta forma de estar e vai requerer que as instituições examinem dados de diversas fontes para quantificar o risco operacional, assim como que observem os diferentes aspectos qualitativos deste risco.

É necessário salientar que o Acordo Solvência II, ainda em fase embrionária, segue, em muitos aspectos, o Acordo Basileia II na forma como está a ser estruturado. O relatório apresentado pela consultora KPMG (KPMG 2002) colocava ainda a hipótese

do risco operacional não ser incluído no documento final, apesar de tal não ser esperado. No entanto, na maioria das suas observações, remete para o estabelecido no Acordo de Basileia para os bancos.

A estrutura do Acordo Solvência II consiste também em três pilares, cada um cobrindo um diferente aspecto dos riscos que as instituições seguradoras enfrentam. O objectivo destes três pilares é alinhar a medição do risco à sua gestão. O primeiro pilar refere-se ao cálculo dos requisitos mínimos de capital que as seguradoras deverão deter para fazer face à sua exposição ao risco operacional. Cabe, assim, às instituições de seguros, deter capital regulamentar suficiente para que estejam protegidas contra eventos adversos (com 99.5% de probabilidade a um período de um ano). O segundo pilar reporta-se a aspectos qualitativos e define requisitos para a governação e gestão de risco nas seguradoras. O terceiro pilar centra-se nos requisitos de apresentação e transparência, através da harmonização do reporte e da informação a fornecer sobre o perfil de risco da instituição. Até à data, a maioria da controvérsia em relação ao Acordo Solvência II tem assentado no cálculo das provisões técnicas e nas fórmulas utilizadas para calcular o capital mínimo regulamentar e o requisito de capital de solvência. Muitos investigadores defendem que há ainda muitos problemas associados ao cálculo de risco operacional para resolver dentro do Acordo Solvência II.

Contrariando a hipótese que foi colocada pelo relatório da KPMG, o projecto Solvência II, em desenvolvimento, irá definir e detalhar questões relacionadas com a gestão do risco operacional. No Acordo Solvência II, o risco operacional foi identificado, por si só, como uma categoria e a sua definição, igual em termos de conteúdo à do Acordo de Basileia II, representa um indicador do reconhecimento, por parte dos supervisores, de que as perdas de risco operacional resultam de interacções complexas e não lineares entre riscos e processos de negócio (Grinsven & Bloemkolk

2009) que é importante identificar, medir e mitigar. Solvência II irá definir um requisito de capital sensível à exposição a risco operacional de cada empresa de seguros. O projecto de Directiva Quadro do Solvência II, actualmente em análise pelo Parlamento e Conselho Europeu, apresenta duas propostas para a quantificação das exposições ao risco operacional: a abordagem standard e a abordagem baseada em modelos internos. A primeira pode levar teoricamente a uma alocação de capital de 20% do valor total do requisito de capital de solvabilidade, apesar de os estudos de impacto QIS3 e QIS4 sugerirem que, na maioria das instituições, este valor vai ser mais baixo. No entanto, continua pouco perceptível a capacidade desta abordagem para conseguir capturar os riscos que a indústria seguradora enfrenta, as especificidades das fontes de risco e, ainda mais importante, os diferentes perfis de risco de cada instituição – a escolha entre modelos internos e a fórmula standard não é simples. A experiência da banca mostra que muitas instituições estão a evitar os modelos avançados, dados os seus custos de implementação e a aparente mais-valia reduzida, associada aos investimentos necessários para o seu desenvolvimento. Enquanto os benefícios tangíveis e intangíveis, que podem ser retirados de uma boa gestão de risco operacional, são visíveis, o valor de cada abordagem para o cálculo do risco operacional continua a representar um objecto de discussão. Independentemente da abordagem seguida, o regulador espera que cada instituição consiga alcançar um nível de compreensão mais elevado dos riscos operacionais a que está exposta.

As empresas de seguros poderão, no futuro, promover e submeter à aprovação da autoridade de supervisão modelos internos para cálculo de requisitos de capital para risco operacional. A mesma Proposta de Directiva estabelece ainda requisitos qualitativos para o sistema de governação, incluindo a existência de um sistema de gestão de riscos. Pelos supervisores da indústria seguradora, será pedido às instituições

que demonstrem que, de facto, compreendem o seu potencial para perdas operacionais; que esses riscos estão dentro dos limites de tolerância e que os planos de mitigação apropriados estão desenhados e disponíveis para serem activados. É, igualmente, expectável que o supervisor solicite às instituições que demonstrem o seu nível de exposição ao risco nas diferentes categorias de risco operacional – incluindo o nível de perdas que a instituição pode suportar em cada categoria.

Neste contexto, convém realçar que, recentemente, o CEIOPS (*Committee of European Insurance and Occupational Pensions Supervisors*) apresentou directivas relativas ao sistema de governação que incluem já algumas ideias sobre a forma como este Comité interpreta a gestão do risco operacional, que servirão, outrossim, de base para o seu aconselhamento à Comissão Europeia quanto às medidas de implementação.

Este Acordo entrará em vigor apenas no ano 2012, porém, o regulador português – Instituto de Seguros de Portugal (ISP) –, admitindo a importância de um sistema adequado para a gestão de riscos, antecipou alguns dos requisitos previstos e avançou com a Norma Regulamentar n.º 14/2005-R, de 29 de Novembro, em que estabeleceu os princípios fundamentais que devem reger a implementação de sistemas de gestão de riscos e de controlo interno nas empresas de seguros, salientando, em particular, a necessidade de gestão do risco operacional; o mesmo normativo estabeleceu um prazo para a implementação dos referidos sistemas, o qual terminou a 31 de Dezembro de 2007.

Neste sentido, as empresas de seguros supervisionadas pelo ISP deverão dispor já de procedimentos e controlos que lhes permitam efectuar uma gestão do risco operacional proporcional à dimensão, natureza e complexidade das suas actividades e riscos. Estes sistemas devem ajudar na compreensão de riscos financeiros e não financeiros a que a instituição está exposta; auxiliar no desenho das estratégias de mitigação e contribuir

para a detecção atempada de falhas ou fragilidades em processos e estruturas operativas. Os sistemas de informação de suporte à gestão de risco operacional devem produzir informação de qualidade, fiável, atempada e relevante acerca das actividades da instituição, dos compromissos assumidos e dos riscos a que a instituição está exposta. A informação veiculada deve ser de fácil acesso, controlo e revisão por meios internos ou externos, devendo também funcionar como um canal de comunicação que assegure o reporte atempado e adequado da informação a todos os intervenientes no processo de gestão de riscos.

2.3.3 – Sarbanes-Oxley

O decreto Sarbanes-Oxley de 2002, também conhecido como Sarbox ou SOX, é uma lei federal dos Estados Unidos da América para responder a um número largo de escândalos corporativos e contabilísticos, dos quais constituem exemplos os que afectaram empresas como a Enron, Tyco International, Adelphia, Peregrine Systems e WorldCom. Estes escândalos, que custaram aos investidores biliões de dólares quando os preços das acções destas empresas entraram em colapso, minaram a confiança mundial nos mercados de capitais. O decreto contém onze secções cobrindo áreas que vão desde as responsabilidades da gestão de topo às penalidades criminais em caso de infracções.

Hoje, continua o debate sobre as vantagens e os custos do SOX. Os seus apoiantes preconizam a imprescindibilidade da legislação, visto que veio desempenhar um papel útil em matéria de restauração da confiança do público nos mercados, através, entre outras medidas, do reforço dos controlos contabilísticos das empresas. Os seus opositores afirmam, em contraste, que este decreto introduziu um ambiente

regulamentar extremamente complexo, que retira competitividade às empresas que o têm de implementar.

Uma das secções mais significativas na área do risco operacional é a secção número 404. Nesta, é requerida à gestão das empresas a produção de um "relatório de controlo interno". Este relatório deve conter uma avaliação de eficiência e eficácia da estrutura de controlo interno e procedimentos – para o fazerem, muitas empresas estão a adoptar a arquitectura de controlo interno descrita na *framework* COSO – *Comittee of Sponsoring Organizations of the Treadway Comission* –, que integra cinco componentes, nomeadamente, Ambiente de Controlo, Assessoria de Risco, Actividades de Controlo, Comunicação e Informação e Monitorização. Esta secção encoraja, assim, as empresas a centralizar e a automatizar os seus sistemas de reporte financeiro, uma decisão fundamentada na melhoria dos resultados obtidos, bem como na esperada redução de custos.

O SOX é uma abordagem orientada para processos, característica que tem vindo a tornar-se comum à quase totalidade das implementações de risco operacional nas instituições financeiras portuguesas. A particularidade da sua orientação para a gestão de risco operacional incentiva a que as linhas orientadoras definidas pelo SOX sirvam também como facilitadoras para novas *frameworks* e metodologias de gestão, como é o caso do BPM (*Business Process Management*), e para a identificação e a implementação de situações de melhoria ou de redesenho de processos.

3 – SISTEMAS DE INFORMAÇÃO PARA RISCO OPERACIONAL

Os sistemas de informação serão um factor primordial para que qualquer instituição consiga implementar programas corporativos de gestão de risco operacional. O âmbito e

os objectivos destes programas representarão os fios condutores para a tomada de decisão relativa aos requisitos de sistemas de informação.

Para que possamos falar sobre sistemas de informação para a área de gestão de risco, devemos primeiro compreender as razões que levam as instituições financeiras a implementar este tipo de sistemas. Para Gibson (1997), podem ser apontadas três necessidades, a saber, a instituição deve (i) ser capaz de medir os riscos a que está ou poderá vir a estar exposta, para entender mais plenamente esses mesmos riscos; (ii) procurar a melhor forma de poder recompensar as unidades de negócio ou os seus colaboradores, ajustando os incentivos à performance na área de risco e (iii) fornecer aos accionistas um *trade-off* óptimo entre risco e retorno.

De acordo com o mesmo autor, a fim de atingir estes objectivos, os gestores começaram por pretender que os seus sistemas de informação de risco lhes possibilitassem quatro funções base: (i) cálculo do VaR, por ser esta a medida universalmente mais difundida e aplicada tanto na área académica como empresarial para avaliação do nível de risco a que uma instituição está exposta; (ii) análise de cenários, o que permite aos gestores, através de simulação aplicada a diferentes factores de risco, a construção de um conjunto de potenciais acontecimentos e a análise do seu impacto na instituição; (iii) cálculo da exposição actual e futura de cada uma das contrapartes, dando assim à instituição uma análise de continuidade do seu perfil de risco; (iv) replicar as funções anteriores por diversos níveis de agregação e dimensões, de forma a conseguir construir informação passível de ser integrada nos diferentes processos de decisão da instituição, a distintos níveis organizacionais.

É, nos dias de hoje, universalmente aceite que, para gerir risco, uma instituição financeira precisa de sistemas de informação sofisticados. Com vista a atingirem os objectivos para que são implementados, estes sistemas devem conseguir combinar

informação de diversas fontes através de um processo estruturado, de modo a estimar o risco a diversos níveis de agregação, e ter a capacidade de reportar os resultados a toda a instituição. Para tal, os sistemas devem estar configurados para responder à especificidade de cada tipo de risco, mas para todos eles deve incluir as seguintes funções base (Kingsley et al. 1998): (i) ter a capacidade de avaliar a perda potencial para as actividades correntes da instituição, bem como para fazer a previsão para novas oportunidades de negócio; (ii) conseguir identificar as causas ou fontes de risco que podem implicar a perda; (iii) apontar os factores que determinam a falha nos controlos que levam à perda e (iv) apresentar informação histórica relativa ao tipo de perda em análise como, por exemplo, casos semelhantes ou indicadores de tendência.

Este conjunto de funcionalidades base ainda permanece actual. No entanto, o desenvolvimento da tecnologia, em conjunto com a evolução dos mercados e da investigação em risco operacional, veio alargar o conjunto de funcionalidades que perfazem, hoje, requisitos no âmbito de implementações de sistemas de informação para gestão de risco operacional. Kross (2009) sustenta que, no contexto de uma iniciativa corporativa de gestão de risco operacional, é de esperar encontrar um sistema (i) que encapsule a estrutura de risco operacional da instituição, incluindo políticas internas e avaliações segundo diferentes abordagens; (ii) que permita capturar factores de risco operacional através de questionários e/ou da análise de indicadores-chave, bem como da recolha de dados estatísticos de diferentes indicadores de risco operacional; (iii) que mantenha uma base de dados de perdas internas, passível de integrar dados externos e dados de auto-avaliações para construir uma distribuição de perdas para a instituição; (iv) que tenha interfaces com sistemas operacionais de risco como, por exemplo, o sistema para cálculo de requisitos de capital; (v) que consiga integrar os seus dados com os sistemas internos e externos de reporte, tais como sistemas de contabilidade ou

sistemas de reporte para a supervisão e, finalmente, (vi) que faculte uma arquitectura para a recolha sistemática de dados e o desenvolvimento de iniciativas e análises da gestão de risco operacional na instituição, com vista à avaliação da sua efectividade e custos associados.

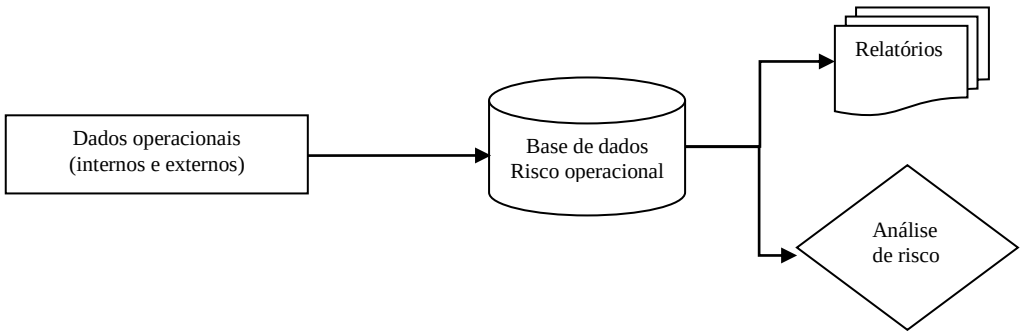
Ainda que, nas etapas iniciais do seu desenvolvimento, os sistemas de informação para gestão de risco operacional se tenham debruçado sobre a resposta aos requisitos impostos pelos supervisores, a sua evolução tende a assumir uma arquitectura que servirá, igualmente, para orientar os colaboradores em direcção aos objectivos essenciais da estratégia de gestão de risco operacional, tendo em conta, outrossim, a estratégica global da instituição. A tendência crescente para agregar, nestes sistemas, áreas como a Auditoria Interna e o *Compliance* revela o objectivo claro de tornar este sector num ponto central, à altura de garantir que a instituição cumpre com a sua estratégia dentro das normas e dos níveis de risco definidos, tanto interna como externamente.

Existe ainda um conjunto de desafios únicos para a análise de risco operacional. O processo de estimar, de entre uma considerável variedade de riscos, o seu impacto e a sua frequência não é tarefa fácil. A abordagem sistemática à gestão de risco operacional irá requerer um sistema capaz de recolher informação, medir e controlar todo um conjunto de riscos que as empresas têm de enfrentar (Mestchian 2003).

O desenvolvimento de sistemas de informação para risco operacional em instituições financeiras ainda é muito recente e o menos avançado das diferentes áreas de risco (as áreas de risco de mercado e de crédito estão já a ser cobertas por sistemas de informação bastante robustos). No entanto, os mais novos desenvolvimentos em áreas como a modelação de dados e a quantificação de risco operacional levaram à promoção de um conjunto de blocos (Figura 5 – Arquitectura de um sistema de informação para

risco operacional) que já poderão ser aplicados à implementação de sistemas de informação para a gestão de risco operacional em instituições financeiras. Algum deste conhecimento foi recolhido em implementações de sistemas noutras áreas, como é o caso da indústria química que demonstra uma vasta experiência na aplicação de sistemas de informação de risco operacional.

Figura 5 – Arquitectura de um sistema de informação para risco operacional



Como já se mencionou, estes sistemas foram desenvolvidos com o objectivo essencial de responder aos requisitos das entidades supervisoras e, para tal, foram concebidos com um conjunto de funcionalidades base visando essa resposta. Assim, estes sistemas permitem a recolha de dados internos – tais como eventos de perdas, avaliações de risco e indicadores de risco e controlo – e a sua integração com dados externos de diferentes consórcios num repositório único de informação de risco operacional. Sobre esta base de dados de risco operacional, os sistemas permitem a construção de diversos indicadores, estatísticas e metodologias de análise de risco com o intuito de responder aos requisitos do pilar I do Acordo Basileia II, ou para permitir à gestão tomar consciência dos riscos a que está exposta e decidir sobre as estratégias de mitigação a adoptar. Por fim, estes sistemas possibilitam o desenho de um conjunto de

relatórios que deverão responder ao que são os requisitos do supervisor, ao abrigo do pilar III, bem como facultar à instituição toda a informação que lhe proporcione tomar as suas decisões operacionais e estratégicas. Um ponto-chave que estes sistemas também deverão garantir passa pelas funcionalidades relativas ao pilar II do Acordo de Basileia II, tais como a sua auditabilidade e a segregação de funções dentro do próprio sistema.

3.1 – Os Dados

Modelos analíticos, metodologias de medição e controlo e todos os métodos e ferramentas criados para os diferentes riscos baseiam-se numa fonte comum: informação acerca de perdas reais e potenciais (Kalhoff & Hass 2004).

Os dados permanecem como o maior obstáculo para uma gestão efectiva de risco operacional. A sua heterogeneidade (diferentes tipos de risco produzem eventos com informação também diversa) e, em certos casos, a sua escassez (falta de uma cultura corporativa que incentive a recolha de dados) tornam o processo de construção de uma base de dados de risco operacional numa tarefa que apresenta muitos desafios novos para as instituições financeiras. A ausência, até aos dias de hoje, de métodos consistentes para lidar com o risco operacional tem causado a inexistência de bases de dados de eventos de perdas – prevê-se que este problema se mantenha, inclusivamente, nos próximos anos (Haas & Kaiser 2004).

Os registos de perdas, que nos casos dos riscos de mercado e de crédito se encontram bem documentadas e existem em número elevado, são escassos no tocante ao risco operacional - as perdas encontram-se mal documentadas e dispersas por toda a instituição, o que se deve ao facto de estas dados não estarem, até recentemente, a ser

recolhidas de uma forma estruturada na maioria das instituições. A necessidade de uma metodologia estruturada para recolha e tratamento de dados relativos a eventos e factores de risco irá permitir às instituições alcançar alguns dos objectivos definidos pelo supervisor, bem como objectivos internos de melhoria operacional (Mestchian 2003). Este processo fornecerá, assim, uma base global à instituição para estimação de risco operacional em processos, recursos, áreas de negócio, ou noutras dimensões. Esta base suportará o desenvolvimento de novos produtos, sistemas e áreas de negócio, através de uma estimação realista de riscos potenciais antes desse desenvolvimento, em vez de os aceitar após acontecerem. Ao agregar riscos de diferentes áreas, processos e recursos dentro da instituição, tornar-se-á possível implementar um ponto central de diagnóstico de causas de falhas e determinar acções correctivas transversais. Todos estes pontos irão permitir, em conjunto, validar a competência operacional da instituição financeira, tanto interna quanto externamente, e, no caso particular da supervisão, garantir que a instituição está a estabelecer uma arquitectura de gestão de risco operacional; que possui a capacidade para reconhecer os riscos a que se encontra exposta e aplica esse conhecimento às suas actividades diárias e estratégicas.

De acordo com Mestchian (2003), para a construção da base de dados de risco operacional, as instituições financeiras podem recorrer a seis diferentes fontes de dados: (i) dados dos sistemas operacionais da instituição – estes são dados que já estão disponíveis em outros sistemas da empresa e que devem servir como fonte de informação para risco operacional; temos, por exemplo, a informação relativa a quebras de sistemas informáticos, que normalmente se encontra registada em ficheiros próprios para cada aplicação; a contabilidade ou a auditoria interna perfazem também áreas de onde se poderão recolher dados relativos a perdas ou a não conformidades e que podem servir como fonte de informação para o sistema de risco operacional, ou como parte do

processo de reconciliação contabilística para validar a capacidade da organização para captar e contabilizar eventos; (ii) dados de eventos internos – dados que, apesar de não estarem armazenados em bases de dados, podem ser recolhidos com o recurso a aplicações desenvolvidas para o efeito; não é comum existir, por exemplo, informação organizada e consistente relativa à falha de processos numa instituição financeira, mas essa informação deverá, no entanto, passar a ser obtida através de aplicações que têm que estar preparadas para recolher os dados de diferentes eventos e armazená-los para futura exploração, incluindo, como já mencionado no ponto anterior, o acesso e a reconciliação aos dados da contabilidade da instituição; (iii) "*self-assessment*" – quando for necessário ter uma ideia de frequências e severidades com que determinados eventos podem ocorrer, mas para os quais não se possui dados suficientes para análise, dever-se-á recorrer a informação qualitativa; apesar de não existir informação relevante para análise relativamente à fraude interna ou externa, é comum haver na instituição o conhecimento necessário para se poderem assumir pressupostos sobre os valores esperados para eventos fraudulentos; (iv) dados externos – hoje em dia, existe um conjunto de consórcios que se encontram a desenvolver bases de dados de eventos de risco operacional passíveis de utilizar como mais uma fonte de informação para o sistema (e.g. FSA, em Inglaterra); importa, no entanto, ressalvar que a utilização desta informação está condicionada à realidade das empresas onde os eventos foram recolhidos e à sua adequação à empresa onde serão aplicados; (v) análise de cenários – para eventos com baixa frequência é necessário um período muito longo de observações a fim de que se logre fazer qualquer tipo de análise estatística; um método à altura de superar esta situação passa pela criação de dados através da construção de cenários; esta abordagem utiliza o conhecimento de gestores experientes e de peritos em gestão de risco para obter avaliações consistentes da frequência e severidade para eventos

específicos; (vi) KRI – estes factores reflectem mais directamente a qualidade dos ambientes operativos e de controlo da instituição, ajudando a alinhar as avaliações de capital com os objectivos da gestão de risco e reconhecendo as melhorias e deteriorações do perfil de risco operacional de uma forma mais imediata.

Um dos problemas mais complexos aquando da tentativa de recolher dados é a sua indisponibilidade. Muzzy (2003) destaca este problema, argumentando que "qualquer pessoa que se aventure na gestão de risco operacional aprende depressa que o processo está condenado ao fracasso se não se tiver dados robustos". Tal deve-se, por norma, à inexistência de dados de perdas referentes a operações internas.

A questão do fraco número de eventos registados de risco operacional é provocada por dois tipos de causas fundamentais. A primeira causa tem como base a falta de uma cultura de risco operacional nas instituições. Uma vez que não existia, até muito recentemente, esta cultura, os métodos ou as ferramentas para que os eventos de risco operacional pudessem ser de alguma forma registados, conjugados com o desconhecimento partilhado pela maioria dos colaboradores das instituições sobre a razão e valor para tal registo, levavam à inexistência de bases de dados para risco operacional; as que existiam serviam, apenas, o risco de mercado ou o de crédito. A segunda causa tem como raiz a falta ou desconhecimento do conceito de risco operacional dentro das instituições, o que implicava que muitos eventos passíveis de serem classificados como risco operacional não o eram, sendo, no entanto, registados em outros sistemas, como é o caso da Contabilidade. Um dos grandes desafios que se colocam, hoje, às instituições é o de conseguir recuperar estes eventos de outros sistemas e classificá-los como risco operacional, incluindo toda a informação a eles associada – por exemplo, quando a contabilidade regista uma perda, não é guardada

informação como data de descoberta, a categoria de risco ou os controlos que falharam, dados, estes, essenciais ao processo de gestão de risco operacional.

Uma solução que tem sido apontada (inclusive pelos supervisores) para esta indisponibilidade de dados é o aumento dos dados internos com dados externos de eventos que ocorreram noutras instituições. Segundo Rao e Dev (2006), a conjunção dos dois tipos de dados envolve dois processos: escala, por ter em conta as diferenças de dimensão, e adequação, por considerar as diferenças de estrutura de negócio. Enquanto Wei (2007) argumenta que os dados externos são extremamente úteis para eventos raros, tornando possível modelar a cauda das distribuições, Frachot e Roncalli (2002) defendem que a conjunção de dados de severidade internos e externos se traduz num processo complexo devido à dificuldade em conhecer a metodologia utilizada na recolha dos dados externos. Os mesmos autores também preconizam que esta conjunção tende a resultar em distribuições pautadas por um optimismo exagerado.

Outro problema reside nos obstáculos únicos colocados pela tentativa de modelação de dados de eventos públicos, entre os quais se destaca o facto de nem todas as perdas serem reportadas ao mercado, enviesando a amostra disponível. Fontnouvelle et al. (2006) advogam que, se a probabilidade de uma perda operacional ser reportada cresce com o aumento da severidade, irá haver um número desproporcional de perdas elevadas relativamente às perdas de severidade baixa nas bases de dados externas. Allen e Bali (2004) sugerem que as bases de dados de risco operacional tendem a sofrer de uma má representação nos eventos de baixa e alta frequência (os de baixa frequência por serem considerados excepções / casos quase únicos, os de alta frequência por, em muitos casos, serem vistos como consequências normais dos processos de negócio e não como erros ou falhas). Já Haas e Kaiser (2004) sustentam que estes mesmos eventos, que, por definição, têm uma probabilidade muito mais baixa de ocorrerem, são normalmente

classificados como confidenciais e, assim sendo, ou não são reportados ou são erradamente classificados como perdas decorrentes de risco de crédito ou mercado, por exemplo, no caso do risco de crédito, os acontecimentos relacionados com o Credit Lyonnais que, entre 1980 e 1999, incorreu em perdas avultadas devido a falhas no seu processo de empréstimos, ou, no caso do risco de mercado, os eventos que levaram à falência do Banco Barings em 1995, os quais foram, numa primeira fase, catalogados como riscos de mercado devido a terem como base operações no mercado de capitais – este ponto torna evidente a dificuldade que pode existir em estabelecer uma fronteira entre os três riscos (na opinião do autor esta tarefa deve, numa primeira fase, ser da competência do supervisor).

Também o recurso a dados obtidos através de análise de cenários e indicadores pode não ser uma solução para o problema, já que se torna extremamente complicado ajustar os cálculos para factores qualitativos e, por outro lado, ainda não existe uma fundamentação teórica sólida para este procedimento (Rao & Dev 2006).

Mas, mesmo no caso de a instituição decidir de forma estratégica começar um processo de recolha de dados, existem problemas relacionados com o próprio processo, ou inerentes aos próprios dados (Haas & Kaiser 2004) - a fraca classificação, ou a falta de informação detalhada são as causas mais comuns. Em relação aos problemas relacionados com o processo de recolha, devemos destacar, como mais usuais, os seguintes: (i) efeito de uma "cultura de risco", que levou as instituições, mesmo ao nível interno, a esconder os seus erros, em vez de os reportar; (ii) dificuldades em classificar / separar os eventos de risco operacional dos de mercado e de crédito – até à existência formal de uma definição de risco operacional apresentada por Basileia II, muitos eventos de risco operacional foram classificados como risco de crédito ou mercado, de acordo com a natureza de operação que lhe dava origem; (iii) alguns eventos podem só

ser detectados meses ou anos depois de ocorrerem – desta forma, só irão alterar o perfil de risco num período muito subsequente. O mesmo é passível de acontecer com eventos que são detectados na altura em que ocorrem, mas cujas consequências financeiras não se podem estimar nesse momento; (iv) certos eventos, como a quebra de sistemas informáticos, não podem ser directamente ligados a perdas financeiras – a sua perda tem de ser estimada recorrendo a outras técnicas como, por exemplo, a estimativa dos proveitos que não se realizaram devido à ocorrência do evento, ou os custos associados à recuperação ou à substituição do sistema afectado.

No processo de recolha, existem opções que podem influenciar, de forma significativa, não só este processo, como as análises feitas sobre os dados recolhidos. Uma destas opções incide sobre o limite abaixo do qual os eventos não são detectados / registados. Esta opção deve-se essencialmente a custos (financeiros e de recursos) associados ao próprio processo de recolha: enquanto este limite desce linearmente, o custo da recolha sobe exponencialmente (Haas & Kaiser 2004). Há uma natural facilidade em recolher os eventos mais extremos, de baixa frequência e alta severidade, não apenas porque são de detecção mais clara, mas por a informação a eles associada se encontrar fortemente documentada. Já os eventos de elevada frequência e baixa severidade não são detectados em razão de, muitas vezes, passarem despercebidos, ou serem vistos como situações esperadas nos processos de negócio. Esta circunstância obriga a que, para que se proceda ao seu registo, a instituição aloque recursos para esta detecção e para a recolha de toda a informação vital ao registo completo do evento. O estabelecimento deste limite é uma opção que irá exercer impacto não só nos custos de recolha e nas medidas de mitigação e controlo, mas também ao nível do cálculo de capital (e.g. distribuição de perda sobrestimada).

Um caso particular deste problema são os eventos de "quase perda" (*near misses*) – perdas não monetárias, ou eventos que, por um conjunto de circunstâncias alheias aos processos ou sistemas de controlo, ao ocorrerem, não implicaram uma perda para a instituição. O registo destes eventos é, muitas vezes, negligenciado devido à falta de formação dos utilizadores acerca deste conceito, o que leva a que, na sua maioria, estes eventos não sejam identificados ou reportados, desfalcando a organização de informação fulcral à identificação de riscos potenciais, de áreas de intervenção ao nível do controlo interno e de acções de melhoria. A instituição deve responder a este problema através de planos de formação que abordem este conceito, capacitando os seus colaboradores com conhecimento que lhes permita identificar e reportar, de forma clara, este tipo de eventos.

3.1.1 – Dados Internos

A utilização de dados internos por parte das instituições de crédito é um pré-requisito essencial ao desenvolvimento e à funcionalidade de um sistema de medição de risco operacional credível. Os dados internos de perdas são cruciais para a aderência das estimativas de risco das instituições à sua experiência real de perdas; representam um requisito para os supervisores, não só como fonte para o cálculo de capital para metodologias avançadas, mas também ao abrigo do Pilar II, no âmbito da demonstração por parte dos bancos e seguradoras de que estão a recolher informação sobre o seu processo interno de gestão de risco operacional. De acordo com o relatório apresentado pela consultora KPMG (KPMG 2005), a recolha sistemática de informação de perdas de risco operacional perfaz uma base fundamental ao desenvolvimento e validação de métodos quantitativos, bem como ao suporte das auto-avaliações qualitativas e como

sistema de aviso de risco. Estas perdas são factores-chave para identificar causas de risco, para construir medidas de mitigação e avaliar a sua efectividade.

As medidas de risco operacional geradas internamente e usadas com o propósito de responder aos requisitos de capital definidos pelo regulador devem basear-se em dados recolhidos num período mínimo de cinco anos, quer esses dados de perdas internas sejam usados para calcular o valor de perda, quer para o validar – quando a instituição opta, pela primeira vez, pela abordagem AMA, é aceitável um período de três anos de dados históricos.

Mais do que por razões de supervisão, os dados internos de perdas tornam-se relevantes sempre que se encontram ligados a dimensões como as actividades de negócio correntes da instituição, aos processos tecnológicos e aos procedimentos de gestão de risco – a existência de dados internos deverá centrar-se menos na modelação de risco e mais na sua utilização para melhorar processos de controlo interno que visem a redução do impacto associado a essas perdas. Cabe, assim, à instituição documentar bem estas dimensões, de forma a avaliar a relevância dos dados de perda históricos, incluindo o impacto de determinados tipos de risco nos seus objectivos parciais ou globais.

De acordo com o Comité de Basileia (BCBS 2003) e com Mestchian (2003), os processos de recolha de dados de perdas internas da instituição devem respeitar as seguintes linhas orientadoras: em primeiro lugar, (i) a instituição deverá ser capaz de mapear os seus dados históricos de perdas internas, conforme as categorias de risco relevantes definidas no primeiro nível do Acordo Basileia II, e fornecer essa informação às entidades supervisoras sempre que solicitado. Deve ser documentado o critério objectivo de alocação das perdas a uma linha específica de negócio e tipo de risco. No entanto, é deixado à instituição decidir até que ponto esta alocação se deve aplicar no

seu sistema interno de medição de risco operacional. Em segundo, (ii) os dados de perdas internas devem ser compreensíveis, capturando todas as actividades materiais e exposições de todos os subsistemas e localizações geográficas. A instituição deve ser capaz de justificar que qualquer actividade ou exposição que tenham sido excluídas, quer individualmente, quer em combinação, foram-no porque não exerceriam impacto material nas estimativas de risco global – a instituição deve ter um limite mínimo de perda para recolha de dados internos. O limite apropriado pode variar entre instituições e, intrinsecamente, por linha de negócio ou por tipo de perda – limites particulares devem ser amplamente consistentes entre dimensões semelhantes. Em terceiro lugar, (iii) conjuntamente com a informação de montantes de perda total, a instituição deve recolher informação sobre a data do evento, quaisquer recuperações ocorridas e informação descritiva das causas do evento de perda. O nível de detalhe de qualquer informação descritiva deverá estar associado ao valor do montante de perda total. Outra linha orientadora passa pela necessidade de (iv) a instituição desenvolver critérios específicos de atribuição de dados de perdas que surjam de um ou mais eventos relacionados, ao longo do tempo, numa dada função centralizada (e.g. num departamento de informática), ou de uma actividade que cobre mais do que uma linha de negócio. E, finalmente, no tocante a (v) perdas de risco operacional relacionadas com risco de crédito e incluídas na base de dados de risco de crédito da instituição (tais como, falhas na gestão de colaterais), estas devem continuar a ser tratadas como risco de crédito no propósito do cálculo de capital mínimo regulamentar e não serão assunto para o capital de risco operacional. Não obstante, e com a finalidade de gestão interna de risco operacional, as instituições devem identificar todas as perdas materiais de risco operacional consistentes com o âmbito da definição de risco operacional, compreendendo aquelas relacionadas com risco de crédito – as perdas materiais de risco

operacional relacionadas com perdas de risco de crédito devem ser sinalizadas separadamente, dentro da base de dados de risco operacional da instituição. Neste ponto, o Comité de Basileia foi, na opinião do autor deste trabalho, redutor ao não atribuir a mesma ênfase ao risco de mercado que conferiu ao risco de crédito, o que conduziu a que algumas instituições financeiras não incluíssem eventos operacionais de risco de mercado nas suas bases de dados. Hoje, a maioria das instituições financeiras já garante, porém, igual tratamento para as duas categorias de risco no seu processo de recolha de eventos.

Os dados das perdas reflectem as ocorrências históricas de risco operacional na instituição e são, na maioria dos casos, recolhidos manualmente por pessoas que estiveram envolvidas na sua ocorrência. Incidem principalmente sobre erros pessoais, tais como a introdução errónea de dados, ou um factor influenciador (e.g. falha dos controlos), e, por isso, desencadeiam receios de uma possível sanção, o que se acaba por reflectir em reportes pobres, especialmente no tocante a perdas de média e grande dimensão. Embora a relação entre o número, a dimensão das perdas e o montante respectivo de capital de risco (usando a abordagem da distribuição de perdas) seja bastante complexa, é do senso comum que, quanto maiores e mais frequentes são as perdas, maior será o capital em risco, causando potenciais consequências negativas para a mitigação e reputação. Sem motivações pessoais de ordem intrínseca para as revelar, existem todos os incentivos para ocultar essas perdas, tornando, consequentemente, ainda mais complexa a quantificação do risco operacional. Assim, este processo deve envolver o estabelecimento de incentivos para a recolha de perdas, determinar a transparência a todos os níveis da instituição e estabelecer um processo sancionatório para situações que não cumpram com normas internas e externas. Um processo de recolha de perdas deve incluir um determinado número de incentivos e controlos para

assegurar um nível elevado de cobertura e qualidade. A própria natureza do risco operacional, ao ser encarado como algo resultante de factores negativos, diminui a vontade de reportar perdas, o que equivale, muitas vezes, à razão que subjaz à falta de qualidade nos dados.

A resolução deste problema tem sido endereçada, com o recurso a diferentes métodos, consoante a instituição financeira. Duas das abordagens mais comuns são (i) a recompensa salarial associada à capacidade de identificar e registar eventos ou riscos operacionais e (ii) a penalização, na avaliação do colaborador, pela incapacidade de participar ou por descurar as suas actividades na gestão de risco operacional da instituição. Seja uma das supramencionadas, seja qualquer outra, todas as abordagens a aplicar devem ter por base um plano de formação estruturado para criar nos colaboradores uma visão clara da importância do programa de gestão de risco operacional para o presente e o futuro da instituição, bem como do papel que cada um desempenha nesse programa.

Tipicamente, quando um evento de perdas internas é identificado, deve ser incorporado um conjunto de informação no seu registo que compreenda, nomeadamente, o seu estado (potencial/ em curso/ concluído), localização, duração, impactos económicos e não económicos dos eventos, bem como a forma como esses eventos foram identificados e as perdas mitigadas. Os registos de eventos devem incluir, outrossim, descrições detalhadas das lições aprendidas e as medidas a tomar para prevenir ocorrências futuras.

Apesar de serem os mais facilmente identificáveis, é comum, nas bases de dados internas, a existência diminuta, ou mesmo a inexistência de eventos de baixa frequência e alta severidade – eventos passíveis de colocar em risco a sobrevivência da instituição, mas que, devido a serem causados por factores extremos, poderão nunca ter ocorrido

nessa instituição, durante vários dos seus ciclos económicos. A falta de massa crítica deste tipo de dados torna as bases de dados internas inapropriadas para modelar eventos com estas características, o que, juntamente com os requisitos impostos pelo Comité de Basileia II para a metodologia AMA, gera, nas instituições, a necessidade de recorrerem a bases de dados externas de eventos de risco operacional – a agregação das duas fontes de dados (internas e externas) de forma a reduzir problemas de enviesamento da distribuição de perdas vai ser um dos principais problemas que se coloca neste processo, e para os quais são, de seguida, apresentadas algumas técnicas para a sua resolução.

3.1.2 – Dados Externos

Embora a sua utilização perfaça um requisito de Basileia II, o sistema de gestão de risco operacional da instituição deve utilizar dados externos relevantes (tanto públicos, quanto oriundos de consórcios), especialmente quando se constatem razões para acreditar que a instituição está exposta a perdas infrequentes, mas potencialmente severas, ou quando existe uma consciência da incapacidade interna para a identificação de determinados tipos de riscos. Além de serem utilizados em análises quantitativas, os dados externos concorrem para indagar se a existência de controlos permite ou não uma efectiva protecção contra certos eventos e se os mecanismos de reporte se mostram suficientes para detectar tais eventos. Informação de natureza mais qualitativa, obtida através de auto-avaliações, pode ser validada, igualmente, através de dados externos, contribuindo assim para refinar a identificação e gestão do risco operacional.

Estes dados externos devem incluir informação acerca dos montantes actuais de perdas, da escala das operações de negócio onde o evento ocorreu, das causas e circunstâncias dos eventos de perdas e, ainda, de outros elementos que contribuam para

avaliar a relevância do evento de perda para outras instituições. Na sua utilização, os dados externos enfrentam, contudo, o desafio do seu nível de representatividade, de forma a serem qualificáveis para uma correcta integração com as bases de dados internas. A qualidade da informação recolhida, a abrangência de linhas de negócio, os processos e as categorias de risco e a adequação entre as realidades das diferentes instituições nas quais os dados foram recolhidos e a da instituição onde vão ser integrados, todos estes problemas exigem que o processo de importação de dados externos seja objecto de uma metodologia rigorosa. O Acordo de Basileia II, ao requerer às instituições financeiras a inclusão de informação externa fornecida por diversos consórcios, apontou, em especial, um conjunto de premissas a considerar no processo de integração, de modo a evitar distorção na base de dados da instituição (Haas & Kaiser 2004), a saber: (i) a não existência de relações lineares entre a dimensão da instituição e a severidade das suas perdas operacionais – terá de haver um mapeamento que estabeleça a correspondência correcta entre os eventos de bases de dados externas e categorias de risco e as linhas de negócio da instituição; (ii) outro problema que afecta as bases de dados externas assenta na circunstância de estas serem usualmente compostas por perdas que foram publicitadas, de forma por vezes compulsiva, nos meios de informação. O consórcio que está a recolher estas perdas deve ter entre os seus objectivos garantir que a informação que vai ser disponibilizada apresenta um elevado nível de fiabilidade e representatividade. No entanto, ao assegurar que as perdas maiores e mais espectaculares estão documentadas, as bases de dados destes consórcios tendem a estar enviesadas para este tipo de perdas, deixando de fora aqueles eventos mais comuns, mas menos “interessantes”, que não circulam normalmente fora dos meios de comunicação internos das instituições.

Dados de perdas externas, isto é, perdas operacionais ocorridas noutras instituições, são recolhidos por diversos consórcios de dados, ou adicionalmente compilados por empresas com fins comerciais. Até à data, os consórcios de dados mais conhecidos são o GOLD (Global Operational Loss Data Base) na Grã-Bretanha e o ORX (Operational RiskData eXchange association) na Suíça. Um exemplo de uma iniciativa nacional é o DIPO (Database Italiano delee Perdite Operative), um consórcio fundado pela associação bancária italiana ABI (Associazione Bancaria Italiana) no ano de 2000 – no final de 2003, os membros do consórcio incluíam 32 bancos ou grupos de bancos. Por norma, a confidencialidade entre os membros e informação estritamente anónima equivalem aos factores primordiais para o desenvolvimento de um consórcio de dados. Isto pode levar a restrições relativamente à profundidade da informação, por exemplo, certo tipo de informação pode revelar com facilidade a fonte de dados, especialmente se o número de membros é baixo. Outros problemas relacionados com o uso de dados externos correspondem à sua classificação e escala. Perdas facilmente suportadas por uma instituição podem ameaçar, em contraste, a sobrevivência de outra instituição. Diferentes factores podem ser utilizados como escala, por exemplo, folhas de balanço, custos e proveitos, ou outros considerados relevantes para diferentes linhas de negócio.

A instituição deve munir-se de um processo sistemático para determinar as situações nas quais os dados externos devem ser usados e as metodologias a utilizar para incorporar esses dados (escalonamento, ajustamentos qualitativos). Estas condições e práticas do uso de dados externos devem ser regularmente revistas, documentadas e sujeitas a revisão periódica independente. Samad-Khan et al. (2006) apresentam algumas linhas orientadoras para quando se integram dados externos, das quais se destacam: (i) a escolha não subjectiva, mas empírica do factor de escala; (ii) a escolha, ou não, de perdas externas de acordo com a sua ocorrência dentro da instituição – as

instituições que operem em determinadas áreas de negócio estão expostas aos riscos dessas mesmas áreas, quer as perdas desses riscos tenham ocorrido quer não no passado; (iii) não efectuar selecções baseadas em critérios de similaridade de linhas de negócio ou geografias e (iv) considerar o facto de não existirem estudos empíricos que permitam mapear a qualidade e os efeitos do ambiente de controlo interno de cada instituição na frequência ou severidade das suas perdas.

Enquanto ferramenta qualitativa, a informação de perdas externas é valiosa para os gestores de risco. Se existirem incidentes significativos – especialmente factores que originaram ou contribuíram para as perdas –, os gestores podem aplicar esse conhecimento às suas operações e, ao combinarem dados internos com dados externos, desenvolver o perfil de risco da instituição que se identifique melhor com a realidade do ambiente em que está inserida. Cagan (2005) afirma que a utilidade dos dados externos estará constantemente presente, mesmo quando as instituições financeiras tenham processos estruturados e globais de recolha de perdas. Os dados externos tornam-se úteis para que os gestores travem conhecimento sobre situações enfrentadas por outras empresas e os utilizem para análise e transformação em casos de estudo – existe uma atitude muito menos defensiva todas as vezes em que se discutem situações ocorridas noutras instituições.

3.1.3 – *Self-assessments*

O objectivo de uma arquitectura de risco operacional é identificar, avaliar, controlar e mitigar este risco, bem como desenvolver reporte efectivo e enfrentar desafios emergentes. A metodologia de auto-avaliação (*self-assessments*) constitui um elemento integral desta arquitectura, pois fornece uma excelente oportunidade para as instituições

integrarem os processos de identificação de riscos e o programa de gestão de risco de uma forma mais geral, com vista a melhorar a compreensão e o controlo dos seus riscos operacionais. Os *self-assessments* podem ser utilizados igualmente como um método para identificar falhas em controlos passíveis de ameaçar a concretização de objectivos de processos ou de negócio e controlar as medidas que a gestão está a desenvolver a fim de reduzir estas falhas. Com base nos seus resultados, podem ser construídos planos de acção para mitigar riscos e melhorar controlos. Apesar das mais-valias associadas aos *self-assessments*, a sua aceitação por parte dos supervisores e por normas de governação corporativa é, ainda, o que tem vindo a impulsionar a sua utilização como meio para recolha de dados de risco operacional.

De acordo com o *Institute of Operacional Risk* (2010), um programa interno de *self-assessments* desdobra-se nos seguintes elementos: (i) a identificação de objectivos de negócio, quer o seu alvo aponte para resultados, quer para a melhoria de processos; (ii) o reconhecimento de riscos que podem ameaçar o alcance desses objectivos e as actividades e processos susceptíveis de serem afectados pelos diferentes riscos que forem identificados; (iii) a identificação e avaliação dos controlos implementados para mitigação de risco operacional; (iv) a determinação de responsabilidades para a execução destes controlos e (v) a avaliação da efectividade dos controlos activos e do nível de risco residual após o controlo.

A escolha da abordagem utilizada por cada instituição para implementar *self-assessments* deve ter em conta aspectos como o seu modelo de governação, cultura, ambiente operacional, dimensão, complexidade e estrutura interna. Estes aspectos podem, segundo o *Institute of Operacional Risk* (2010), direccionar as instituições para a implementação de uma de três abordagens: (i) abordagem baseada em *workshops*, passível de ajudar a ultrapassar aspectos mais burocráticos, normalmente associados a

estes processos, mantendo a capacidade de capturar a informação mais relevante. Esta abordagem é um mecanismo que logra captar uma maior aderência e disponibilidade dos colaboradores para falarem dos seus riscos, controlos e partilharem iniciativas de melhoria. Os *workshops* trazem benefícios para a consciencialização sobre os riscos que exercem impacto em diferentes processos e níveis da instituição; perfazem, outrossim, excelentes mecanismos de transferência de capacidades internas de gestão de risco e de implementação de controlos de difícil medição (e.g. comunicação interna ou formação). Os (ii) questionários correspondem a uma das abordagens mais utilizadas pelas instituições e a que está mais divulgada. Tipicamente, as perguntas colocadas versam sobre temas como a relevância dos processos e a frequência e severidade de diferentes tipos de riscos. Questões acerca da existência de controlos e sua efectividade são também comuns em programas mais avançados de gestão de risco operacional. Quando bem construídos, estes questionários podem criar valor, pois permitem melhorar o conhecimento sobre os perfis e responsabilidades na gestão de risco operacional em cada área da instituição, propiciam a identificação dos riscos que a instituição enfrenta, incluindo a sua frequência e impacto, e possibilitam avaliar o risco residual ou não mitigado, através da comparação entre a performance dos controlos implementados e o que está definido pela instituição enquanto valor "óptimo" de controlos internos. Por fim, (iii) a abordagem híbrida engloba, numa primeira fase, o recurso a um *workshop*, seguida de um conjunto de questionários de avaliação e acompanhamento. *Workshops* adicionais podem tornar-se necessários, em casos de surgimento de novos requisitos de negócio que desempenhem um impacto significativo na instituição.

Os dados resultantes do processo de *self-assessment* potenciam um valor considerável no processo de gestão de risco operacional. No entanto, a sua combinação com outros dados eleva ainda mais a sua importância. Esta combinação com dados de

eventos internos pode gerar indicadores valiosos como, por exemplo, a indicação de áreas susceptíveis, nas quais possam ocorrer no futuro eventos de risco operacional, ou a comparação dos resultados da frequência e severidade registados nos questionários e os reais registados na base de perdas internas. Estas análises representam indicadores relevantes a propósito da qualidade de ambos os processos de recolha de dados, além de servirem de linhas orientadoras para o processo de gestão de controlos e medidas de mitigação.

Maugrado as vantagens apresentadas, erguem-se críticas à coerência e exactidão dos resultados obtidos através desta metodologia. Com base na sua investigação no campo da psicologia do julgamento e da tomada de decisão, Daniel Kahneman e Amos Tversky (1972) avançaram com alguns dos problemas mais graves quando é pedido ao ser humano para apresentar estimativas sobre determinado fenómeno, tais como a tendência para ver padrões em fenómenos aleatórios, a maior sensibilidade a certos tipos de riscos, a propensão para acreditar mais em pequenas amostras (ignorando a sua variância) do que em maiores e a insensibilidade a probabilidades anteriores.

Os *self-assessments* equivalem a uma entre as várias metodologias de recolha de informação para fornecer às instituições uma arquitectura mais coerente e integrada no seu programa de gestão de risco operacional, sendo uma das mais apresentadas por supervisores e organismos consultivos, como o Acordo Basileia II ou o SOX.

3.1.4 – Análise de cenários

Segundo o Acordo de Basileia II, as instituições bancárias devem utilizar a análise de cenários, juntamente com dados externos, para avaliar a sua exposição a eventos de baixa frequência e alta severidade, ou para identificar riscos potenciais cuja ocorrência

ainda não se verificou ou que ainda não foram detectados pelos sistemas de controlo interno. A análise de cenários pode também ser usada para avaliar o impacto de divergências de suposições de correlação, embutidas na estrutura de medição de risco operacional da instituição, em particular para avaliar perdas potenciais que surjam de múltiplos eventos em simultâneo. Este facto guarda uma maior relevância porque é comum que os processos de recolha de dados de risco operacional, quer por eventos, quer por questionários de auto-avaliação, sejam efectuados de forma isolada, no contexto de um departamento, unidade de negócio ou de uma situação particular, perdendo assim a visão transversal a toda a organização.

Bilby (2008) define análise de cenários como um processo sistemático para obter a opinião de gestores de negócio e gestores de risco, a fim de construir uma avaliação "razoável" da frequência e impacto de determinadas perdas de risco operacional plausíveis. A análise de cenários cria uma estrutura para a compreensão de fenómenos transversais que, ao exigir o entendimento de fenómenos mais complexos e a intervenção de diferentes estruturas da instituição, irá permitir corrigir informação anteriormente recolhida em situações mais isoladas, sem a visão global do seu impacto.

A análise de cenários, um elemento imposto pela abordagem AMA, serve para identificar possíveis eventos de alto impacto que não ocorreram até à data. Em contraste com a recolha de dados de perdas, concentrada exclusivamente no passado, a análise de cenários enfatiza aspectos orientados para o futuro do risco operacional. Existe uma ligação íntima entre análise de cenários e testes de stress, dado que a identificação analítica e empírica de cenários extremos é um pré-requisito para realizar testes de stress.

As análises de cenários, realizadas no contexto de gestão de risco operacional, encerram objectivos quantitativos e qualitativos. Entre os objectivos quantitativos,

destacam-se a capacidade de complementar os dados usados para o cálculo de risco – através de dados relativos a eventos extremos, que deverão ser utilizados para a modelação da cauda da distribuição de perdas e na construção das bases para conduzir testes de *stress*. Os cenários deverão incluir situações críticas para a análise do seu impacto na instituição. Os objectivos qualitativos centram-se no desenvolvimento de uma perspicácia nos riscos horizontais, ou seja, devem permitir avaliar riscos que poderão ser transversais em diferentes processos e ter impacto em diferentes unidades de negócio. Os cenários criados devem permitir: (i) a análise de riscos que ocorrem ou têm impacto em diversas áreas da instituição, compensando, assim, a visão da recolha de dados de eventos internos que enfatiza riscos que sucedem e exercem o seu impacto num ponto específico da estrutura organizacional; (ii) a descoberta antecipada de riscos – através do desenvolvimento de cenários e da análise dos seus impactos, a instituição consegue identificar riscos potenciais que não lhe são facultados pelas formas mais tradicionais de recolha de dados, tais como o registo de eventos internos ou os questionários de auto-avaliação; (iii) a identificação das fraquezas da instituição – em concerto com o ponto anterior, a análise de cenários permite identificar falhas em processos de controlo ou na capacidade da instituição para mitigar eventos de risco operacional, potenciando, deste modo, informação vital para que se possam gerar estratégias pró-activas de gestão de risco operacional e ideias para a optimização de processos; muita da informação recolhida na análise de cenários pode ser utilizada para aperfeiçoar os processos da instituição, através da melhoria do seu desenho, evitando eventos potenciais de risco, ou embutindo neles medidas de mitigação que permitam reduzir perdas financeiras ou outro tipo de impactos plausíveis.

3.1.5 – Indicadores de Risco

Adicionalmente ao uso de dados de perdas, sejam actuais, sejam baseadas em cenários, a metodologia de avaliação de risco da instituição deve capturar indicadores de ambiente de negócio e factores de controlo interno que alterem o seu perfil de risco operacional. Os KRI's (*key Risk Indicators*) continuam a ser, a par da análise de cenários, uma das áreas de menor desenvolvimento nas instituições financeiras. No entanto, de acordo com Davies et al. (2006), o investimento em programas de KRI's irá produzir benefícios em áreas como o estabelecimento de limites de exposição ao risco (a análise do histórico dos indicadores pode sinalizar padrões de evolução de negócio e do risco associado, bem como da eficácia e eficiência de controlos e medidas de mitigação que poderão ser utilizados no estabelecimento de limites), optimizar estratégias de risco versus retorno e melhorar a probabilidade de a instituição atingir os objectivos de negócio, através de uma mais efectiva gestão de risco operacional.

Os indicadores-chave são estatísticas, ou métricas, que podem fornecer evidência acerca da habilidade da instituição para gerir e mitigar riscos, ou de como o risco se está a modificar ao longo do tempo. Estes indicadores passam a ser chave quando conseguem, com alto nível de eficácia, identificar situações de elevada importância para a instituição, sendo o reporte do perfil de risco dirigido aos órgãos de gestão; antecipar perdas extremas; apontar áreas onde é possível reduzir a exposição ao risco operacional e comunicar os diversos níveis de exposição a risco de diferentes processos – perfazem estas algumas das principais razões que motivam as instituições financeiras a implementar programas de indicadores de risco.

Apesar da sua manifesta utilidade, a aplicação destes indicadores tem enfrentado alguns problemas, dos quais se destacam a capacidade de demonstrar que estes

indicadores conseguiram realmente identificar potenciais perdas; a consistência da sua utilização em diferentes linhas de negócio; a sua incorrecta definição e especificação e a capacidade de os integrar e agregar numa estrutura que permita a sua recolha sistemática.

Para garantir o uso efectivo dos indicadores de medição de risco, existem algumas regras que devem ser consideradas na sua implementação: (i) a escolha de cada indicador deve ser justificada como um factor significativo de risco, baseado na experiência e no envolvimento de colaboradores com um elevado nível de conhecimento nas áreas de negócio afectadas; sempre que possível, os factores devem ser traduzidos em medidas quantitativas passíveis de verificar; (ii) a sensibilidade das estimativas de risco da instituição à mudança nos factores e o peso relativo de cada indicador devem ser bem argumentados: além de capturar mudanças de risco devido a melhorias em controlos, os indicadores devem apreender, outrossim, aumentos potenciais no risco, devido à maior complexidade dos processos ou ao aumento do volume de negócio; (iii) os valores destes indicadores, incluindo o suporte justificativo para qualquer ajustamento das estimativas empíricas, deve ser documentado e sujeito a revisão independente dentro da instituição e por parte das entidades supervisoras; (iv) com o passar do tempo, o processo e os seus resultados têm de ser validados através do confronto entre a experiência de perda interna actual, dados externos pertinentes e ajustes realizados.

Ao encontro do que foi exposto nos pontos anteriores, os indicadores-chave de risco de uma instituição financeira devem fornecer informação de perdas reais e potenciais, tornando possível a identificação antecipada de áreas de risco mais elevado, bem como identificar tendências que permita que estes indicadores se transformem em sistemas de alertas para situações tendencialmente prejudicais aos objectivos institucionais. Na

selecção dos indicadores a implementar, a instituição deve perceber quais as áreas de maior risco para cada uma das suas unidades de negócio, para depois escolher indicadores que cumpram os pontos já identificados. Alguns dos indicadores mais comuns são: taxa de flutuação de pessoal; dias de licença por doença; horas extra; número e duração de falhas de sistema; resultados de auditorias internas; frequência de reclamações e entradas contabilísticas erradas. Os indicadores que forem seleccionados devem ser claramente documentados, de forma a garantir a transparência e a clareza na sua interpretação e implementação; deve ser-lhes igualmente aplicada uma estrutura de limites que faculte o seu controlo e acompanhamento, a fim de que a instituição reaja (aceitando ou mitigando), de acordo com a sua estratégia de gestão de risco operacional, às diferentes variações que os valores destes indicadores vão assumindo ao longo do tempo. Não existe um número certo de KRI's a manter por cada instituição, esta decisão deve basear-se no nível de heterogeneidade de riscos dentro da instituição em causa e da sua capacidade de gestão de números maiores ou menores de KRI's.

Os sistemas de indicadores-chave de risco pretendem ser sistemas de advertência, com vista a prevenir perdas, potenciando a tomada de decisões de mitigação pró-activa. Associados a estes, encontram-se também os indicadores de controlo (KCI), que incidem sobre a eficácia e eficiência dos mecanismos de controlo da instituição e a capacidade desta para mitigar risco operacional recorrendo a controlos internos (e.g. erros detectados por reconciliação contabilística, tentativas de intrusão informática) – a sua definição e escolha devem seguir os mesmos critérios relativos à relevância e clareza dos seus objectivos. Em conjunto, estes indicadores criam um elemento importante de uma *framework* de risco operacional integrada, que irá permitir, à instituição, a verificação da correlação entre perdas e indicadores de risco, para a confirmação dos valores de recolha e análise, bem como a manutenção de um sistema

de alerta em tempo real, com vista à identificação de situações potenciais de risco que possam afectar a estratégia ou a própria sobrevivência dessa instituição.

3.1.6 – Bases de dados

A criação de bases de dados para risco operacional tem sido motivada por dois factores (Moosa 2008): (i) requisitos da supervisão e (ii) gestão de risco operacional. As bases de dados de perdas internas são usadas para registar e classificar eventos de perdas, bem como os resultados dos processos de auto-avaliação, os valores dos indicadores de risco e as análises de cenários. A recolha sistemática desta informação dentro da instituição forma a base para uma análise de situações de risco e, subsequentemente, para controlo de risco. A qualidade dos modelos de medição de risco operacional também depende fortemente da qualidade dos dados registados na base de dados.

Sendo os dados a base do sistema de informação, estes representam igualmente a fonte de alguns dos problemas plausíveis mais graves, por exemplo a não disponibilidade ou aplicabilidade dos dados, comum à maioria dos sistemas de informação. Existem, no entanto, questões próprias da área do risco operacional passíveis de afectar a construção da base de dados (Marshall 2001), a saber: (i) as perdas podem ser politicamente sensíveis – para gerir os riscos operacionais retirar-se-á preferencialmente o máximo da informação possível acerca das perdas, incluindo informação detalhada caso a caso; todavia, algumas considerações legais, como protecção dos dados e segurança de dados de clientes e empregados, podem restringir o nível de pormenor permitido; (ii) a falta de dados para eventos pouco frequentes, o que cria a necessidade de integração de dados externos ou análises de cenários; (iii) a

utilização de dados externos, apesar de necessária, cria problemas associados à sua aplicabilidade às situações e ambiente de negócio específico da instituição; (iv) a integração de dados externos com dados internos, que, como foi visto anteriormente, é um processo que acarreta alguns desafios complexos; (v) a integração de diferentes abordagens de modelação, o que implica a necessidade de diferentes tipos de dados e diversos níveis de desagregação; (vi) dificuldade de modelação do comportamento humano, visto que o risco operacional se relaciona bastante com fenómenos que resultam de atitudes de colaboradores, clientes e outros actores dos mercados em que as instituições operam. A informação necessária para tentar compreender os riscos envolvidos e para os modelar é muito dependente do risco que se analisa e das abordagens que se aplicam; (vii) a dinâmica do risco operacional faz com que este acompanhe de perto a evolução dos mercados e as mudanças que ocorrem tanto interna quanto externamente, o que provoca que a realidade dos factores, tipos de risco, frequência e impacto dos eventos de risco operacional também esteja em constante mutação.

Outros problemas organizacionais podem surgir durante o processo de implementação da base de dados: (i) a definição de quem deverá ser responsável pelo registo da informação – se deve ser dado acesso a todos os colaboradores, ou se devem existir responsáveis de risco operacional dentro de cada uma das unidades de negócio; (ii) quem é que deve deter a base de dados – a questão sobre quem deverá ser o detentor da base de dados de risco operacional tem sido colocada em muitas instituições e está intimamente ligada ou a razões históricas (departamentos que já lidavam de alguma forma com os riscos que hoje são classificados na categoria de risco operacional), ou a questões de reporte (unidades que são responsáveis pelo reporte ao supervisor), ou, ainda, às direcções responsáveis pelas actividades de controlo interno dentro da

instituição; (iii) a capacidade de classificar correctamente um evento de risco operacional – devido à ausência de formação ou esclarecimento interno, ainda se verifica uma certa inconsistência na forma como deverão ser classificados os eventos de risco operacional, o que induz o não registo de eventos que deveriam ser registados, o registo de situações que deveriam ter sido classificadas como risco de crédito ou mercado, ou o registo de toda e qualquer situação que seja considerada um erro ou falha; (iv) a data em que os eventos são registados – é crítico que os eventos sejam registados logo que descobertos; existe, porém, a tendência para serem acumulados e só posteriormente registados, no final de determinados períodos (e.g. fim do mês), ou registados somente quando já exista toda a informação para fechar o evento (e.g. perda final, recuperações). As perdas operacionais têm frequentemente um historial e um ciclo de vida, isto é, não se confinam a um único ponto no tempo, pelo contrário, desenvolvem-se gradualmente. No entanto, o registo de perda apenas na data final do seu fecho pode ter impactos severos na gestão da instituição, já que a pode deixar, durante longos períodos, sem informação vital sobre os riscos nas suas operações e processos (e.g. um evento de fraude externa deve ser registado logo que detectado, evitando assim tentativas semelhantes).

Power (2005) identifica, em todo o processo de recolha de dados, aspectos comportamentais que exercem implicações no volume e na qualidade da informação que fica registada na base de dados. Afirma que existem, por exemplo, fortes razões para não reportar eventos de impacto significativo, caso impliquem o crescimento da carga de capital aplicada à unidade de negócio que reportou o evento (mais perdas implicam normalmente maior alocação). Por outro lado, as perdas podem ser sobrestimadas como parte do argumento para assegurar mais recursos para a unidade.

De acordo com Mossa (2008), existem três princípios essenciais à construção de uma base de dados para risco operacional, cuja presença garante o cumprimento dos requisitos do supervisor e a solidez das análises e decisões internas de gestão de risco operacional: (i) cobertura, ou seja, uma infra-estrutura capaz de capturar eventos ao longo de toda a organização, quer sejam aspectos técnicos, quer de processo; (ii) totalidade, princípio que se refere à capacidade de apanhar todas as perdas acima do nível definido e com toda a informação requerida e (iii) correcção da informação registada – devem ser mantidos processos de qualidade de dados para garantir que os dados registados representam fielmente os eventos que ocorreram.

Um dos aspectos mais sensíveis para o sucesso da gestão de risco operacional assenta na actualização frequente e na utilização eficiente das bases de dados, antes que novos processos e sistemas sejam introduzidos na empresa. Da mesma forma, e de acordo com as novas exigências das entidades reguladoras, todos os processos de criação e manutenção destas bases de dados devem estar claramente documentados, de modo a garantir, a todos os intervenientes no sistema de informação, a coerência e relevância da informação nele contida. Assim, existem aspectos metodológicos a considerar no processo de constituição de uma base de dados para risco operacional, a saber: (i) a base de dados deve estar preparada para suportar alterações na instituição e nas estruturas de controlo ao longo do tempo; (ii) "standards" de dados são essenciais para a consistência na captura de dados; (iii) os dados devem ser capturados por linha de negócio, enquanto "input" importante de perfil de risco (Basileia II, Solvência II); (iv) para maximizar o valor da informação, as perdas devem ser recolhidas por linha de negócio e processo e manter o detalhe necessário, de modo a que a instituição possa aprender com eventos passados e "*near misses*"; (v) dever-se-á utilizar dados externos para complementar a base de dados de perdas internas.

A expressão "*garbage in, garbage out*" sugere que, relativamente aos dados, muito planeamento e estandardização devem ser aplicados no contexto de qualquer modelo de dados viável, a fim de assegurar a qualidade dos dados utilizados nas diferentes análises. A necessidade de "standards" para os dados é um aspecto muito importante nas bases de dados internos e externos, começando pela necessidade de estabelecer uma definição consensual de risco operacional. Esta definição vai determinar que tipos de eventos serão apropriados para a base de dados. Algumas questões que se levantam relativamente à padronização da base de dados traduzem-se nas seguintes orientações: (i) que perdas serão incluídas? Para responder a esta pergunta, tem de existir um dicionário de dados no qual se define "perda operacional" e se delimita, explicitamente, cada classe e subclasse; (ii) decidir que standard aplicar na entrada de dados em cada um dos campos, por exemplo, campos de datas, de moeda, de localização geográfica e de texto; (iii) definir e associar uma classe de risco standard a cada item – tem de haver uma definição clara de cada classe de risco, de modo a que os códigos sejam precisos; (iv) determinar e perceber a amplitude e largura dos dados que se estão a recolher, para que se traduzam uniformes ao longo de todos os registos; (v) empregar nomes uniformes para todos os departamentos, negócios e produtos, a fim de que possam ser agregados por debaixo de um nível superior; (vi) ter um campo para a fonte de informação (pessoa, gestor, reporte periódico, etc.) e (vii) documentar todas as datas, incluindo aquela em que o registo deu entrada, e um campo de comentário para observações futuras.

Na construção de uma base de dados de perdas de risco operacional, uma das questões que mais veementemente se levanta, devido ao seu impacto no próprio processo de recolha de dados, é a definição do que realmente constitui uma perda de risco operacional. Segundo o Acordo Basileia II, apenas as perdas directas devem ser

registadas, sendo a justificação para esta restrição a de que estes efeitos são objectivos e passíveis de medir de forma consistente. A outra questão (já anteriormente apresentada) prende-se com o limite abaixo do qual as perdas não serão registadas. A escolha deste limite é uma questão de custo e benefício devendo, por isso, ser efectuada de acordo com as linhas de negócio, de instituição para instituição.

Quanto aos dados a recolher relativos a cada perda, em KMPG (2005) identificou-se os seguintes: valor bruto, recuperações por seguros e outras, categoria de risco, linha de negócio em que ocorreu a perda, data de ocorrência e data de descoberta, áreas de negócio responsáveis pela gestão da perda e causas do evento. Moosa (2008) aponta outro conjunto de dados a registar a propósito da ocorrência de um evento de risco operacional, nomeadamente a área onde foi detectado o evento e o utilizador que o reportou (este ponto é de elevada sensibilidade devido a todo o peso emocional que normalmente se associa ao processo de reportar eventos de risco operacional), bem como o estado do evento, ou seja, se este ainda está em aberto (i. é, ainda não terminou a sua ocorrência, ou não existem dados finais sobre o seu impacto), ou se já se encontra fechado, incluindo todas as datas associadas a cada um destes estados.

Além de responderem aos que deverão ser os objectivos internos para a gestão de risco operacional, os dados a recolher devem também ir ao encontro dos requisitos do supervisor para a abordagem seleccionada. Das diversas implementações estudadas neste trabalho, foram identificados os seguintes campos como os mais comuns nas bases de dados: datas (evento de perda, detecção, entrada nos livros contabilísticos); severidade da perda (perda total); valores ajustados, provisões e *write-offs*; compensações relacionadas com perdas; recuperações; tipo/categoria de risco; linha de negócio; localização geográfica; empresa do grupo; unidade organizacional; descrição, especificando causas significativas dos eventos de perdas, e referência a risco de

mercado ou crédito. Existem outros conjuntos de dados potencialmente enriquecedores para a descrição de um evento que podem ser igualmente reconhecidos. Apesar de alguma desta informação não ser de fácil recolha na altura do registo do evento, a instituição deve empreender esforços para que esta seja recolhida e complemente o dossier do evento. Alguns dos dados a recolher passam pela resposta a perguntas como (Levine 2007): (i) Quais os controlos associados a esse evento? (ii) Que factores subjacentes levaram à perda? (iii) Resultou a perda de falhas em controlos ou da cultura corporativa da instituição? (iv) Existe alguma correlação entre o período de ocorrência e o montante da perda? (v) É possível afirmar que, quanto mais tempo um determinado risco demorou a ser detectado, maior o foi montante da perda? (vi) As estratégias de financiamento de risco, tais como os seguros e planos de investimento para financiar perdas, foram efectivas? (vii) As diferenças culturais internacionais constituíram factor a considerar?

Existem também especificações que têm de ser garantidas para que os requisitos definidos pelo supervisor e os objectivos de reporte sejam alcançados como, por exemplo, o respeitar do mapeamento dos eventos para os tipos de risco e das linhas de negócio exigidos pelo supervisor. Com vista a acomodar as possíveis mudanças de requisitos por parte dos supervisores, as bases de dados devem ser desenvolvidas com base em modelos que apresentem um elevado nível de flexibilidade, de modo a terem em conta tais mudanças. A informação que é introduzida na base de dados deve seguir procedimentos de aprovação para o registo de perdas – a entrada de dados de perdas deve ser verificada e aprovada. Associada a esta temática, está a questão de segregação de funções, o que implica que a instituição mantenha uma estrutura interna de risco operacional que garanta que os processos de registo, validação, consulta e gestão de

toda a informação na base de dados são feitos dentro das normas de segregação de funções estabelecidas pelo supervisor.

Um aspecto fundamental na construção de uma base de dados para risco operacional é a capacidade de recolha de dados de forma automática de outros sistemas de informação da instituição. Uma das fontes de dados sobre incidentes actuais ou possíveis consideradas excelentes são as reconciliações, a saber, reconciliação entre os sistemas financeiros e entre os sistemas de crédito e de mercado, reconciliações com entidades não financeiras e entre as várias fontes de dados operacionais. Outra fonte de dados surge da análise dos sistemas transaccionais e de pagamento. Nestes sistemas, podem recolher-se dados de diversos eventos, dos quais são exemplo instruções falhadas, transacções não confirmadas ou não comparáveis e outros eventos referentes ao não cumprimento da regulamentação em vigor, impliquem estes eventos ou não perdas reais. Os eventos em questão podem apresentar causas tão distintas como a introdução no sistema de dados incorrectos, a falta de informação relevante (e.g. prazo final do contrato), mapeamentos incorrectos ou definição errónea das regras de negócio, modelos inexactos e falhas de sistemas.

O maior obstáculo à construção da base de dados é o subdesenvolvimento da cultura de risco – conceito, necessidade e vantagens da gestão de risco operacional –, o que encorajou, por muitos anos, os colaboradores das instituições a fornecerem demasiados relatórios positivos de riscos e a esconderem dos respectivos superiores erros e potenciais perdas. Assim, para recolher dados fiáveis de perdas e indicadores-chave de risco e garantir a realização de análises de cenários e auto-avaliações de uma forma correcta, deve ser criado um sistema de incentivos que permita e motive os colaboradores para colaborem neste processo de modo transparente, sem receios e conscientes de que a informação que se dispõem a fornecer imprimirá um impacto

significativo na forma como a instituição que integram conduz os seus negócios e nos resultados que vai obter.

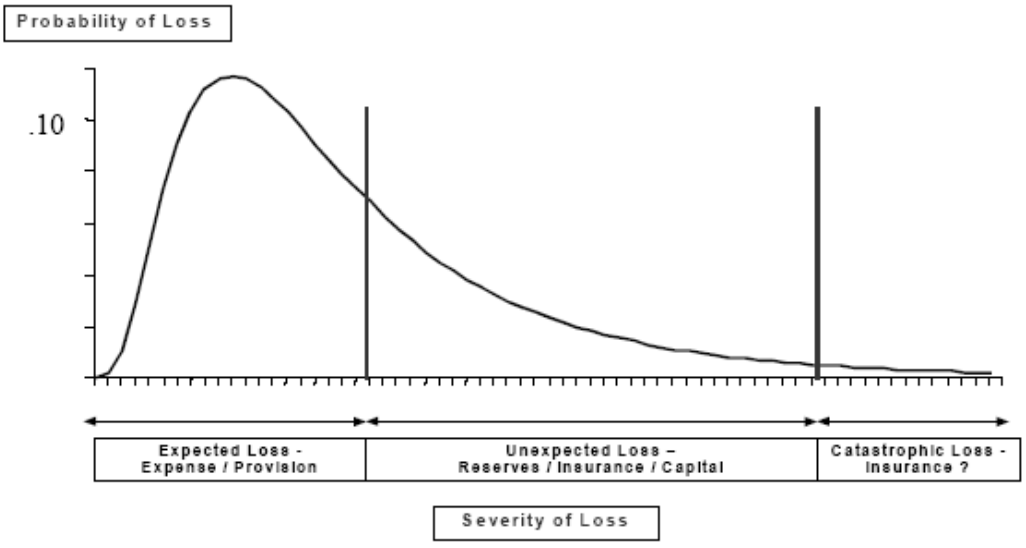
3.2 – Modelação e quantificação de Risco Operacional

Os modelos de risco operacional englobam uma variedade de modelos estatísticos e econométricos desenhados para calcular o capital regulamentar, ou capital económico a alocar para risco operacional, assim como para estudar causas e consequências. No entanto, Bhatia (2002) argumenta que a medição de risco operacional não é apenas motivada por incentivos de menor alocação de capital regulamentar, mas também porque permite às instituições implementar auditorias baseadas em indicadores de risco, suporta uma cultura de consciencialização do risco e admite a identificação de linhas de negócio mais rentáveis e de vantagens competitivas. Bocker e Kluppelberg (2005) sugerem que a única forma correcta de gerir risco operacional com sucesso passa pela sua identificação e minimização, o que requer o desenvolvimento de técnicas de quantificação adequadas; Fujii (2005) realça, por sua vez, que a quantificação do risco operacional constitui um pré-requisito para a formulação de uma arquitectura efectiva de capital económico.

A necessidade de exprimir o risco em números é a base de uma das frases mais citadas em gestão de risco, "*you can't manage what you can't measure*". Assim, após se conseguir construir uma base de dados coerente, com informação de qualidade e relevância para a análise de risco operacional, é necessário analisar esta informação de forma a ser possível calcular indicadores da exposição da instituição financeira aos diversos riscos, identificar tendências, ou apontar causas para determinados eventos. O resultado de todas estas análises é fornecer à gestão um conjunto de métricas que lhe

permitam perceber qual o nível de risco a que a sua instituição está exposta, a fim de propiciar a implementação de processos correctivos ou medidas de mitigação (Mestchian 2003). Uma das abordagens mais comuns para modelar risco operacional tem como finalidade construir uma distribuição das perdas potenciais de risco operacional para um determinado período temporal (Figura 6 – Distribuição de perdas operacionais). Tipicamente, esta distribuição é obtida através da combinação das distribuições da frequência e severidade das perdas, o que possibilita obter a medida VaR (*Value at Risk*), que representa o valor que a instituição pode esperar perder a um certo nível de probabilidade (e.g. 99.9%), sendo com base neste valor que esta deve alocar capital para se proteger contra este risco e evitar situações de insolvência.

Figura 6 – Distribuição de perdas operacionais (Fonte: Rosengren 2001)



Uma das abordagens possíveis para classificação dos modelos de risco operacional divide-os em modelos *top-down* e *bottom-up*. Os modelos *bottom-up* baseiam-se na análise de eventos de perda em processos individuais, enquanto os *top-down* começam

no nível de topo da organização e vão descendo para as linhas de negócio. Os modelos *bottom-up* são suportados por dados fornecidos por colaboradores que estão sob avaliação e que têm, por isso, pouco incentivo para serem pró-activos. Há que realçar que estes modelos podem ser utilizados, inclusive, com o propósito de diagnóstico de risco e no desenho de controlos internos, ao passo que os modelos *top-down* podem ser efectivos na estimação de requisitos de capital económico. Currie (2004) defende o uso concorrente de ambos os tipos de modelos para o cálculo de requisitos de capital para risco operacional.

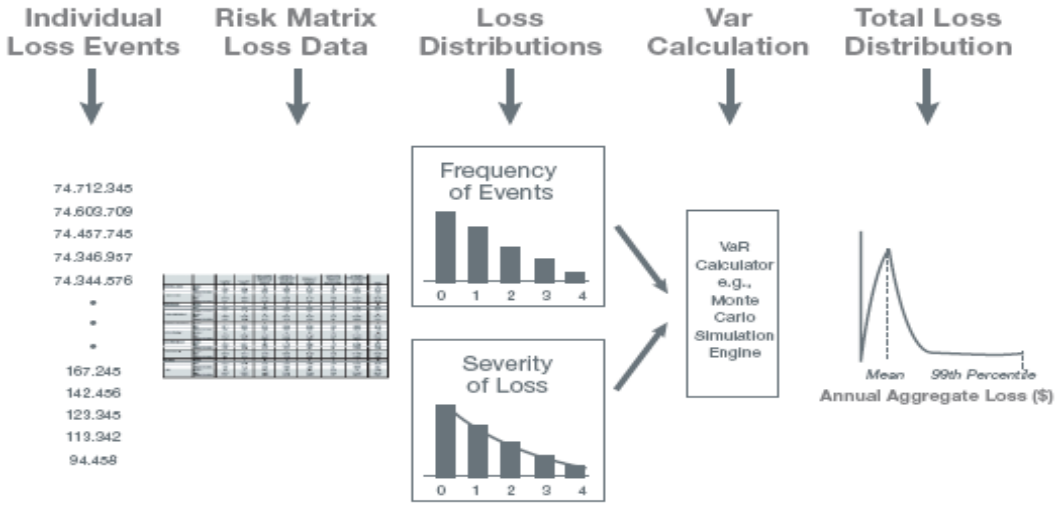
De acordo com Mestchian (2003), várias técnicas têm sido utilizadas para a modelação de risco operacional: (i) modelo económico de *pricing* – um exemplo é a utilização do CAPM (*capital asset pricing model*) para sugerir uma distribuição para o preço do risco operacional, como mais uma componente para determinar o preço do capital. Este modelo tenta atribuir a todos os componentes da valorização da instituição uma categoria de risco, incluindo risco operacional, sendo estes bastante úteis para a medição deste risco ao nível corporativo, utilizando metodologias *top-down* para alocação a unidades de negócio. Apresentam, porém, alguns inconvenientes, como a dificuldade na ligação entre as acções da gestão e as implicações no capital, e revelam uma falta de capacidade para lidar com situações reais de irregularidades. Outra técnica assenta na (ii) análise de cenários – como já mencionado, esta fornece uma ferramenta qualitativa para compreender mais plenamente o impacto associado a eventos operacionais de magnitude elevada, que concorre, outrossim, para o desenvolvimento de planos de contingência para mitigar esses eventos. Um cenário funciona como um guião para uma situação futura, descrevendo uma combinação de eventos potenciais, para os quais é pedido, a um painel de peritos nas áreas de negócio potencialmente afectadas, um conjunto de avaliações (normalmente sobre frequência e impacto dos riscos

identificados). A sua utilização é eficaz no tocante a eventos raros, pois produz informação sobre eventos cujos dados não podem ser capturados estatisticamente, servindo também como um exercício de aprendizagem para situações futuras – esta técnica leva a repensar as assunções das práticas de negócio existentes; sugere, ainda, novas abordagens para situações vindouras, bem como o desenvolvimento de medidas de mitigação para responder a potenciais eventos críticos. No entanto, esta técnica também encerra algumas fraquezas: em primeiro lugar, a escolha dos cenários é arbitrária e sujeita à experiência passada da instituição ou a expectativas sobre os factores de risco do ambiente em que esta se insere; em segundo, esta técnica não dá qualquer probabilidade sobre a possibilidade de ocorrência de cada cenário. Os (iii) modelos estatísticos de perdas equivalem à técnica de modelação de risco operacional actualmente mais utilizada nos sistemas implementados (Figura 7 – Modelo estatístico de modelação de perdas) – nesta, os dados reais são utilizados para construir distribuições de probabilidades da frequência e severidade. Esta técnica apresenta diversas vantagens para a instituição, tais como o facto de os resultados se basearem nas características intrínsecas à instituição e evoluírem, ao longo do tempo, de acordo com as medidas de gestão. Os custos e benefícios das medidas de mitigação podem ser analisados e, devido ao facto de se basearem nos mesmos princípios matemáticos do risco de crédito e de mercado, permitem também a combinação estatística destes dois riscos com o risco operacional. Manifesta, todavia, esta técnica, algumas desvantagens, uma vez que se mostra extremamente exigente ao nível do volume e da qualidade dos dados, além de que perfaz, potencialmente, uma abordagem essencialmente centrada na análise do histórico e não numa perspectiva de futuro. Importa atentar, finalmente, na técnica de (iv) modelos de factores – inúmeros factores poderão explicar as perdas operacionais, o que impõe a necessidade de optimizar a sua identificação e de encontrar

possíveis correlações. A análise de factores é uma técnica que, com base num número vasto de variáveis, verifica se estas têm um pequeno número de factores em comum que respondem pela sua inter-correlação. Uma das análises que pode ser utilizada para a modelação de risco operacional é a redução e transformação de variáveis, permitindo identificar um conjunto reduzido de factores que explicam uma percentagem elevada da variância do modelo, o que facilita a gestão e mitigação dos principais factores / causas de risco operacional da instituição.

Um ponto-chave na escolha de uma das quatro técnicas apresentadas é a quantidade e a qualidade dos dados a que o sistema tem acesso: modelos estatísticos ou de factores necessitam de um conjunto substancial de dados internos para efectuarem os seus cálculos; já os modelos de *pricing* e de análise de cenários baseiam mais os seus cálculos no conhecimento dos utilizadores do sistema de informação.

Figura 7 – Modelo estatístico de modelação de perdas



Outra classificação é apresentada por Smithson e Song (2004) em que os modelos de risco operacional são divididos em três abordagens: (i) abordagem de processos; (ii)

abordagem de factores e (iii) abordagem actuarial. Na abordagem de processos, o foco incide sobre os processos individuais que constituem as actividades operacionais, o que significa que os modelos que se classifiquem sob esta abordagem são necessariamente modelos *bottom-up*. Esta abordagem engloba modelos causais, análises estatísticas de controlo de qualidade e "*reliability*", análises de conectividade, redes *baysianas*, *fuzzy logic* e dinâmica de sistemas. Nas redes causais, são construídas redes de nós, cada um representado uma variável aleatória do modelo, que permite estabelecer a relação e o comportamento entre os diferentes componentes, tornando possível, deste modo, conjugar conhecimento de especialistas e dados históricos de forma a possibilitar adquirir uma visão global do problema a modelar e prever as consequências de determinadas intervenções no sistema, tais como, medidas de mitigação ou implementação de controlos. As análises estatísticas de controlo de qualidade, em muito semelhantes à técnica anterior, são usadas de forma abrangente para a avaliação de processos de produção. Na análise de conectividade, a ênfase é depositada nas ligações entre os diferentes componentes do processo.

Na abordagem de factores, procura-se identificar os determinantes significativos do risco operacional, seja ao nível de topo da organização, seja em níveis mais baixos (linhas individuais, de negócio, ou processos). Esta abordagem cobre indicadores de risco, modelos CAPM ou modelos preditivos. Nos indicadores de risco, alguns tipos de regressão, como a exponencial, podem ser utilizados para identificar factores de risco como, por exemplo, o volume das operações, classificações de auditoria e rotatividade de empregados. Os modelos tipo CAPM são usados para relacionar a volatilidade dos resultados com os factores de risco operacional – o risco operacional é calculado medindo os betas do risco de mercado, crédito e outros, e deduzindo-os do beta total. Os

modelos preditivos, a análise discriminante e outras técnicas semelhantes servem a identificação dos factores que levam a perdas operacionais.

A terceira abordagem é a actuarial, cujo foco aponta para a distribuição de perdas associadas ao risco operacional. Wei (2007) argumenta que esta parece ser a escolha natural para a quantificação de risco operacional, através da estimação das distribuições de frequência e severidade de forma independente. A abordagem actuarial cobre as seguintes técnicas: (i) distribuições empíricas de perdas – levantamento de dados internos e externos de perdas dispostos em histogramas de frequência e severidade; (ii) distribuição de parametrização explícita – implica estimar a frequência e severidade da técnica anterior, confluindo ambas para obter a distribuição de perdas efectiva e (iii) a teoria do valor extremo (EVT) – área da estatística para aplicação a comportamentos de dados extremos. Esta teoria é aplicada à modelação dos valores extremos da distribuição de perdas, defendendo que para esta existem algumas distribuições típicas (e.g. distribuição generalizada de Pareto) que permitem apresentar estimativas sólidas sobre a probabilidade de ocorrência de eventos que apresentam uma frequência historica bastante reduzida.

Reynolds e Syer (2003) propõem outra classificação, descrevendo a modelação de risco operacional com uma estrutura baseada em três elementos, a saber: a abordagem de distribuição de perdas (LDA – *Loss data approach*), a abordagem baseada em cenários (SBA – *Scenario based approach*) e a abordagem de indicadores, normalmente designados *scorecards* (SCA – *Scorecard approach*). A base desta classificação é a natureza dos dados necessários para implementar cada uma destas abordagens: enquanto a LDA depende de dados históricos, as outras duas abordagens são prospectivas – dados de probabilidades e severidades futuras são recolhidos através de opiniões de especialistas, recorrendo a análises de cenários ou indicadores.

Haubenstock e Hause (2006) apresentam alguns factores a considerar sempre que uma instituição está a seleccionar a abordagem de modelação. Um dos factores mais importantes é a disponibilidade de dados, especialmente dados históricos referentes a eventos de risco operacional – uma abordagem LDA, por exemplo, não é possível sem um processo robusto de recolha de dados. Também a disponibilidade e o esforço dos recursos alocados à gestão de risco operacional devem ser factores a pesar, já que, enquanto uma abordagem LDA pode ter um impacto mínimo nas unidades de negócio, a análise de cenários é bastante exigente tanto ao nível do número de horas, quanto ao nível de conhecimento requerido aos seus colaboradores. Outro dos factores importantes reside nos incentivos para a gestão do risco – por exemplo, em abordagens SCA, é mais imediata a visualização do impacto dos incentivos internos para a melhoria na gestão de risco. O custo perfaz outro factor vital à escolha da abordagem, pois, em alguns casos, poder-se-ão revelar necessários investimentos em *software* ou serviços de consultoria, ao passo que, para abordagens que apostem mais no conhecimento interno, tais investimentos podem ser significativamente reduzidos. Por fim, a cultura da organização constitui um factor igualmente relevante, porque se encontra intimamente ligada à capacidade da instituição de recolher mais informação quantitativa ou qualitativa. Qualquer que seja a abordagem que se adopte, quanto mais transparente for o processo e melhor captar o perfil de risco da instituição, mais bem aceite será por toda a instituição. Como já foi referido, o Comité de Basileia, nos documentos que apresentou, defende que um sistema de gestão de risco envolve a utilização de dados internos, de dados externos considerados relevantes, a análise de cenários e factores que reflictam o ambiente de negócio e o sistema de controlo interno para a modelação de risco operacional – uma interpretação igualmente sustentada por Giudici (2004).

Tendo modelado o capital a alocar a risco operacional, a instituição torna-se, assim, preparada para alocar capital às diferentes linhas de negócio, incentivando-as, desta forma, para uma gestão e uma redução mais eficientes do seu risco operacional, com o objectivo de minorar o valor que lhes é alocado. De acordo com a metodologia de modelação de risco operacional LDA que tem vindo a ser apresentada, a abordagem que se propõe para estimar o capital a alocar baseia-se nos riscos reais que ocorrem nas operações da instituição (uma abordagem mais simplificada seria a utilização do capital regulamentar). Segundo Marshall (2001), a alocação de capital deve fundar-se numa avaliação completa dos riscos de cada linha de negócio em particular, atentando especificamente naqueles que implicam variação nos resultados através do seu impacto nos custos e nos proveitos da instituição. Esta avaliação é normalmente realizada através ou de dados qualitativos (*self-assessments*), ou de informação quantitativa, como a recolha de eventos de perda. O mesmo autor preconiza três abordagens para o processo de alocação de capital às linhas de negócio: a primeira equivale à (i) contribuição isolada de risco. Nesta abordagem, a linha de negócio é analisada isoladamente, separada por completo do resto da instituição, reflectindo os riscos que estão directamente sob o controlo da gestão dessa unidade de negócio, os quais não podem ser afectados pelas actividades de outras linhas (por esta razão, é esta a abordagem mais indicada para medição de performance pois faz os seus resultados não estão associados a decisões e medidas de outras áreas). Outra abordagem coincide com a (ii) contribuição diversificada de risco. Nesta, a alocação é realizada tendo por base os riscos da abordagem anterior e a correlação do P&L da linha do negócio com o total da instituição, ou seja, é a fracção do risco total da instituição que pode ser alocada de volta a cada linha de negócio (esta abordagem não é indicada para análise de performance, uma vez que as medidas tomadas em outras linhas de negócio podem ter impacto no

capital alocado). Resta realçar a (iii) contribuição marginal de risco. Nesta abordagem, a contribuição de uma linha de negócio é definida como a diferença entre o risco total da instituição com essa linha de negócio e o risco da instituição sem essa mesma linha, o que se torna útil à tomada de decisão referente a opções de investimento ou desinvestimento.

Para assegurar a validade deste processo, deve o supervisor exigir à instituição a revisão contínua dos riscos operacionais a que está exposta, bem como actualizações regulares à sua modelação. Independentemente da forma como as diferentes abordagens são actualizadas, às instituições financeiras será pedido que todas elas estejam bem documentadas, que o peso relativo de cada abordagem para o cálculo de capital seja demonstrável (de componentes tanto quantitativos, quanto qualitativos) e que o modelo de cálculo de capital se baseie em fontes apropriadas, ou seja, que os dados ou cenários utilizados reflictam adequadamente o risco operacional da instituição.

Apesar dos recentes avanços da modelação de risco operacional, existem ainda muitos problemas que tornam complexo o desenho de modelos e métricas extremamente fiáveis para utilizar no processo de gestão das instituições financeiras. Koker (2006) defende, por exemplo, que o risco operacional é difícil de medir devido a duas características: a falta de uma boa *proxy* para a exposição de risco operacional e a cauda pesada da sua distribuição de perdas. Outro problema associado à modelação de risco operacional surge da característica cíclica dos eventos de perdas. Allen e Bali (2004) argumentam que a extrapolação do passado para aferir o risco futuro pode falhar, se existirem factores cíclicos que tenham impacto nas medidas de risco operacional. Embora os dados históricos de risco operacional recolhidos durante períodos de expansão económica possam revelar-se irrelevantes para períodos de recessão, é uma prática habitual ignorar factores cíclicos e calcular uma linha não ajustada de tendência

para o futuro. Os supracitados autores sugerem que os componentes cíclicos de eventos de perda operacional estão correlacionados com flutuações macroeconómicas, enquanto Allen e Turan (2007) fornecem evidências da presença de componentes cíclicos no risco operacional. Outro obstáculo à tentativa de uma visão agregada de risco operacional traduz-se na dificuldade em avaliar o nível de correlação entre diferentes tipos de risco e unidades de negócio, devido à falta de dados históricos.

No caso específico da metodologia AMA (*Advance Measurement Approach*), apresentada pelo Comité de Basileia para a modelação de risco operacional, Moosa (2008) dirige algumas críticas à sua constituição, aos problemas na sua utilização para o cálculo do capital regulamentar e aos custos e benefícios desta metodologia. No que respeita à constituição da abordagem AMA, este autor afirma não existir consenso sobre quais as abordagens (LDA, SBA, SCA) que a devem integrar e de que formas serão combinadas, ou não, entre si para o cálculo do capital regulamentar. A não clarificação desta questão irá pesar sobremaneira no trabalho do supervisor, tendo este já reconhecido que a variedade de práticas utilizadas na modelação poderá mesmo levar a situações em que instituições com um perfil análogo de risco tenham diferentes níveis de alocação de capital para risco operacional. Uma das críticas mais fortes à AMA prende-se com a utilização da métrica VaR como principal indicador de risco.

A utilização do VaR tem vindo a receber muitas apreciações menos positivas, em especial no tocante à sua utilização no risco operacional, devido a ser uma medida que assenta fortemente no pressuposto de normalidade da sua distribuição, pressuposto que raramente se verifica quando se trata da distribuição de perdas referentes a risco operacional. Outras críticas ao VaR são: (i) a sua incapacidade para dar informação sobre a cauda da distribuição de perdas (no caso do risco operacional, tem tendência para ser pesada) – metodologias como o VaR condicional ou a *extreme value theory*

podem ser utilizadas para minimizar esta questão – e (ii) o facto de ser apenas uma indicação sobre o volume de risco e não sobre a sua tipologia (e.g. risco legal, risco tecnológico). Em defesa do VaR há que realçar que muitas das fragilidades que apresenta têm como fonte a fraca quantidade e qualidade dos dados em que assenta, bem como o seu objectivo (é uma medida puramente quantitativa e não tem atributos qualitativos).

Esta metodologia obriga a sérios investimentos, quer em recursos humanos, quer em sistemas de informação, a fim de fazer face a todos os requisitos próprios da metodologia e aos que são exigidos pelo supervisor para que a instituição possa aplicar a abordagem AMA. Estes investimentos podem ser justificados tendo por base o pressuposto apresentado pelo Comité de Basileia, que certifica que as instituições que apliquem a AMA irão registar uma redução do valor de capital a alocar em relação às outras duas abordagens. Mossa (2008) observou, porém, que esta circunstância nem sempre se verifica, estando muitas vezes o resultado dependente dos dados existentes na instituição e da utilização, por parte desta, de seguros para mitigação de eventos de risco operacional, não apresentando, assim, uma forte relação com a estrutura interna de gestão de risco operacional. Como tal, o autor acrescenta que algumas das instituições que optem pela metodologia AMA irão desenvolver e testar vários modelos em regime laboratorial (testar vários abordagens e modelos), com o objectivo primordial de encontrar aquele que minimize a alocação de capital regulamentar e não o que melhor capte o seu perfil de risco.

Um problema fulcral na AMA é a disponibilidade dos dados. Qualquer que seja o conjunto de abordagens utilizadas, todas elas são altamente dependentes de dados, dados esses que levantam uma diversidade de questões, tal como foi apresentado em capítulos anteriores – é necessário reforçar que é neste ponto que as instituições

financeiras que queiram avançar para metodologias de modelação mais avançadas terão que concentrar os seus recursos e investimentos iniciais.

Quando se faz referência a dados para a modelação de risco operacional, o registo de eventos internos são aqueles que apresentam normalmente uma maior relevância. Estes têm por causa inúmeros factores, incluindo erros humanos, problemas técnicos e eventos naturais – todos estes podem ocorrer sem ter por base medidas ou acções internas à instituição. O resultado destes eventos é, em muitos casos, difícil de prever – alguns eventos podem nem sequer ser detectados, e outros não o são devido ao volume da perda daí decorrente não ser relevante. Outro dos problemas já detectados é que, para risco operacional, os reguladores sugerem uma base de um ano para as análises (e.g. cálculo do VaR). Esta indicação pressupõe que o perfil de risco da instituição financeira não sofre qualquer alteração ao longo de um ano. No entanto, a maioria das actividades de gestão têm, claramente, um efeito imediato no perfil de risco da instituição (Kalhoff & Hass 2004), o que pode indicar que a previsão de capital a alocar para efeitos de risco operacional, definida pelo regulador, não garante uma aderência fiável aos riscos operacionais e às medidas de mitigação que ocorrem diariamente numa instituição financeira. A maior complicação reside na linha de corte estabelecida para a recolha de dados. Devido ao custo que implicaria a recolha de toda e qualquer perda de risco operacional, são estabelecidos limites abaixo dos quais não são recolhidas perdas. Assim, quando se constroem modelos recorrendo aos dados internos, haverá a tendência para sobrestimar o risco, devido à sua distribuição ter-se essencialmente baseado em valores elevados de perda (Kalhoff & Hass 2004).

Os modelos apresentados nesse capítulo são os que têm granjeado maior aceitação por parte das instituições financeiras. Existem, no entanto, outros modelos que vêm sendo utilizados para modelação de risco operacional. Young e Coleman (2009) expõem

alguns destes modelos: (i) *Dynamic Financial Analysis* (DFA) – esta abordagem utiliza métodos estocásticos para simular um grande número de cenários, a fim de comparar diferentes estratégias e apoiar na tomada de decisão com base em indicadores de gestão da instituição; (ii) *Bayes Belief Networks* (BBN) – através da construção de diagramas em rede, esta abordagem permite aos gestores terem uma visão do impacto dos seus processos ao longo da instituição e no seu perfil de risco, incluindo a possibilidade de realização de testes de *stress*; (iii) *Data Mining* – a sua utilização é mais comum na modelação não de distribuição de perdas, mas de alguns tipos de riscos operacionais, como é o caso da fraude.

Apesar do valor indiscutível da modelação em risco operacional, a sua utilização pode também contribuir para o surgimento de problemas para o processo de gestão de risco operacional nas instituições. Currie (2004) alerta para algumas das potenciais consequências, não intencionais, da utilização de modelos, com o objectivo de gestão diária de risco operacional, incluindo: (i) sensação de falsa segurança – existindo um modelo que apresenta valores indicativos de perda, a instituição sente-se mais segura relativamente ao valor potencial das perdas reais futuras e não procura outras técnicas para a validação desse valor; (ii) gestão do modelo em detrimento da realidade – todos os recursos são aplicados na recolha de dados para o processo de modelização, em vez de serem aplicados na identificação e mitigações de eventos reais; (iii) mau direccionamento do foco da organização – resultante dos dois pontos anteriores, emerge o perigo de a instituição se concentrar mais no desenvolvimento de métricas e de mecanismos para suportar a modelação do que no controlo e acompanhamento da evolução do perfil de risco dos seus processos de negócio, bem como da sua implicação na estratégia da instituição; (iv) má canalização de recursos – os recursos podem ser alocados de acordo com estimativas de um modelo que pode já estar ultrapassado; a

aplicação dos recursos de acordo com o modelo terá tendência para ser mais reactiva do que preventiva; (v) desencorajamento de "*whistle-blowers*" – é normal que a existência de modelos crie reservas para a apresentação de casos que contradigam os seus resultados; (vi) ignorância cega – como resumo de todos os pontos anteriores, a utilização de modelos pode fazer com que a instituição os veja como o seu único / principal ponto de controlo e de identificação de risco operacional. Esta prática irá implicar que a instituição não se aperceba das limitações do seu programa de gestão de risco operacional e conduza as suas actividades com base em resultados de modelos que apresentam diversos problemas (já apontados), e que, na sua generalidade, não captam o perfil de risco actual da instituição.

A utilização de modelos envolve sempre custos elevados e a alocação de recursos por parte das instituições, o que implica que a sua utilização deverá ser mais ampla do que apenas responder a requisitos do supervisor. A instituição deve acreditar que estes modelos trarão benefícios para a sua gestão diária de risco operacional e que produzirão informação a introduzir nos seus processos de tomada de decisão.

3.3 – Relatórios

Como mencionado no capítulo anterior, o objectivo de todas as análises é disponibilizar um conjunto de relatórios que permita uma melhor gestão do risco operacional. Estes relatórios perfazem elementos fundamentais no processo de comunicação dentro da instituição, permitindo agregar todas as suas estruturas em torno dos objectivos do seu programa de gestão de risco operacional. Estes relatórios irão possibilitar aperfeiçoar, outrossim, os processos de análise de riscos e de detecção de eventos de perda e garantir um acompanhamento eficiente das medidas de mitigação. A

estrutura dos relatórios de risco operacional deve ter como objectivo atingir aspectos críticos do binómio causa / efeito, ou seja, devem estes apresentar de forma clara as causas para os diferentes riscos e os efeitos por eles produzidos transversalmente a toda a instituição. Em instituições mais avançadas quanto à sua arquitectura de gestão de risco operacional, devem ser também descritos os controlos que estão implementados e as medidas de mitigação aplicadas.

Ao contrário da informação referente a risco de mercado ou de crédito, não era comum, até à publicação do Acordo de Basileia II, que as instituições financeiras disponibilizassem internamente ou ao mercado informação relativa à sua exposição a risco operacional, bem como aos procedimentos para a gestão deste risco.

A natureza voluntária do reporte de risco operacional, nos primeiros anos após as propostas do novo Acordo de Basileia, permite obter algum entendimento sobre os potenciais motivos que podem incentivar os órgãos de gestão de uma instituição financeira a apresentar resultados sobre o seu programa de gestão de risco operacional. Um primeiro aspecto a destacar é que o não fornecimento ou o fornecimento insuficiente de informação sobre a gestão de risco operacional pode levar entidades exteriores à instituição a sobrestimar a perda esperada e a probabilidade de realização de um evento de risco operacional, o que conflui, consequentemente, para uma maior exigência de retorno por parte de investidores. Pode, assim, argumentar-se que, num cenário como este, a disponibilização de informação será benéfica, em particular em contextos de bancos que estão preocupados com o seu custo de capital.

Helbok e Wagner (2006) afirmam, com base em diversos estudos, que a apresentação de resultados referentes a risco operacional pode ter impactos nos custos, devido a acções regulamentares, e na redução do custo de capital – o risco operacional é um factor determinante na decisão de atribuição de *ratings* por parte das empresas que

disponibilizam esta informação, o que, directa ou indirectamente, tem impacto no custo de capital das instituições. Os autores colocam a hipótese de que bancos com um rácio de capital e/ou uma taxa de retorno dos activos relativamente baixa escolham um nível mais elevado de apresentação de dados sobre risco operacional. O racional para esta afirmação é que os investidores podem perceber que o impacto de um evento de risco operacional pode ser superior em instituições financeiras menos capitalizadas e menos rentáveis. Assim, estes investidores estarão mais preocupados com a gestão de risco operacional em bancos com estas características, exigindo um nível mais elevado de detalhe na informação apresentada.

Sendo o risco operacional um elemento que depende fortemente da qualidade da gestão e dos recursos da cada instituição (mesmo factores externos, como a fraude, podem ser mitigados através de medidas internas de controlo), é natural que os diferentes intervenientes dos mercados financeiros revelem interesse na informação que cada instituição disponibiliza relativamente a este tópico. Deste modo, a disponibilização de informação também poderá ser utilizada por instituições que se pretendem distinguir mostrando competências ao mercado. Neste cenário, espera-se que as instituições com boa performance sejam as primeiras a avançar para a apresentação de resultados de gestão de risco operacional que lhes permita garantir melhores oportunidades de negócio e captar mais investimento.

No entanto, uma das maiores influências para a apresentação de informação advém das regras e regulamentação criadas pelas entidades supervisoras. De acordo com Watts e Zimmerman (1986), a apresentação de informação por parte dos bancos evita que estes desencadeiem uma atenção não desejada por parte do supervisor. Uma vez que o papel dos supervisores passa por assegurar a estabilidade do sistema bancário, devem estes debruçar-se especialmente sobre bancos com estruturas mais fracas de capital, já

que estas terão mais dificuldade em suportar uma elevada perda operacional, fornecendo assim um incentivo para que estes bancos tenham apostas mais elevadas nos seus processos de apresentação de informação ao mercado.

Em conjunto com os requisitos de capital, o Comité de Basileia tem vindo também a endereçar a questão da apresentação de informação ao mercado, no âmbito do pilar III sobre disciplina de mercado. Isto reflecte a ênfase depositada pelo Comité na promoção da transparência e da efectiva disciplina de mercado, através da apresentação de informação específica sobre risco operacional. Como princípio geral, os bancos devem possuir um procedimento formal de apresentação de resultados aprovado pelo nível de topo das instituições financeiras, que enderece a abordagem do banco sobre que relatórios serão apresentados, quais os controlos internos acerca deste procedimento, assim como um processo para avaliar a adequação dos seus relatórios. Relatórios relativos à gestão de risco têm de incluir os riscos a que as instituições financeiras estão expostas e as técnicas utilizadas para identificar, medir, acompanhar e controlar esses riscos.

Para o risco operacional em particular, existe mais um conjunto de requisitos de reporte de dados qualitativos que consiste: (i) na declaração da abordagem ou das abordagens utilizadas para avaliação de capital a que o banco se candidata e (ii) numa descrição detalhada da abordagem AMA, caso o banco se esteja a candidatar a esta abordagem. Em termos quantitativos, os bancos candidatos à abordagem AMA devem indicar os requisitos de capital referentes a risco operacional, antes e depois de qualquer redução desse capital resultante da utilização de seguros. Além do pilar III, a estrutura do novo Acordo de Basileia inclui, outrossim, o documento "*Sound Practices for the Management and Supervision of Operational Risk*", que contém linhas orientadoras e requisitos que formam a base do processo de apresentação de resultados para risco

operacional.

Para lá dos reguladores, outros organismos responsáveis por definir standards de contabilidade e de governação, bem como empresas de *rating*, estão a endereçar o tema de reporte de risco nos bancos e seguradoras. Estes standards e recomendações de governação corporativa que emergiram recentemente na maioria dos mercados financeiros têm como objectivo elevar o nível de apresentação de informação, de forma a fornecer aos investidores uma imagem abrangente dos riscos existentes e dos conflitos de interesses dentro das empresas cotadas. Nos Estados Unidos da América, o decreto Sarbanes-Oxley de 2002 estabelece standards claros sobre a responsabilidade da gestão pela apresentação de informação e dita consequências, caso esta informação não seja apresentada ou a sua qualidade se revele questionável. Deste decreto, destaca-se a secção 404, que requer informação sobre o sistema de controlo interno da instituição e da arquitectura implementada para o controlar, e a secção 409, que reclama a implementação de sistemas de controlo em tempo real sobre as condições financeiras em que a instituição está a operar.

No Reino Unido, em 2003, a Financial Services Authority (FSA), assim como, na Alemanha em 1996 e 1998, um conjunto de leis enfatizam que todos os colaboradores de instituições financeiras devem estar informados das suas responsabilidades relativas à gestão de risco e apontam especialmente para as responsabilidades globais da gestão de topo, no que concerne a gestão de risco e a disponibilização de informação relevante.

Também as empresas de *rating* estão a incorporar as abordagens das instituições financeiras relativamente à gestão de risco operacional nas suas decisões, mostrando-se particularmente interessadas em saber como as instituições vêm recolhendo a informação sobre eventos de perda. A empresa Moody's (2003), por exemplo, tem, como um dos pilares centrais da sua arquitectura para avaliação de instituições

financeiras, o reporte e a transparência dos processos internos de recolha de dados e a estrutura e procedimentos para gestão de risco.

Da mesma forma que no risco de mercado ou de crédito, bem como em outras áreas que necessitam de informação, existe um conjunto de princípios básicos para a implementação efectiva de relatórios de risco operacional de modo a potenciar a sua gestão. Marshall (2001) afirma que os relatórios necessitam de ser claros, apresentados num contexto, completos, consistentes, centrados no utilizador, produzidos de forma atempada e com o mínimo de redundância, ou seja, cabe aos relatórios identificar as questões que os utilizadores querem ver respondidas e não sobrecarregá-los com informação excessiva ou supérflua. Devem ser contextualizados, para que se possam realizar comparações com outros valores das dimensões de análise (e.g. tempo, processo, linha de negócio), e claros quanto aos pressupostos utilizados para as análises efectuadas. O processo de desenvolvimento destes relatórios deve ser estandardizado dentro da instituição e muito bem documentado, a fim de garantir a consistência na sua construção e interpretação, e a sua disponibilização deve ser realizada dentro de tempos que permita à instituição pôr em prática as suas medidas de mitigação.

Mais do que visando responder ao supervisor, as instituições devem desenvolver um sistema adequado à monitorização e reporte dos riscos a que estão expostas e à avaliação de como a alteração no perfil de risco da instituição afecta as suas necessidades de capital, os seus resultados e a sua relação com os seus colaboradores, accionistas e mercado em geral. Os órgãos de gestão da instituição devem receber, regularmente, relatórios que lhes permitam fazer o acompanhamento de todos estes vectores, para poderem, então, tomar as medidas necessárias com vista a garantir que os objectivos estratégicos da organização são alcançados. Para tal, estes relatórios devem permitir aos decisores: (i) avaliar o nível e a tendência dos riscos materiais e o seu efeito

nos níveis de capital; (ii) apreciar a sensibilidade e a racionalidade de suposições fundamentais usadas no sistema de cálculo de capital; (iii) determinar que a instituição assegura o capital suficiente para os diferentes riscos e que se encontra em conformidade com os objectivos de adequabilidade de capital estabelecido; (iv) avaliar os seus requisitos de capital futuro, baseados nos relatórios de perfil de risco da instituição e realizar os ajustamentos necessários de acordo com o plano estratégico dessa instituição.

Para efectuar o acompanhamento de toda a informação referente às diversas abordagens, perspectivas e análises de risco operacional, os *scorecards* têm sido uma das formas mais utilizadas, já que esta abordagem integra tanto a perspectiva "*top-down*" quanto a "*bottom-up*". Uma das suas grandes vantagens é perfazer um canal de comunicação ideal para ligar causas a acções e às pessoas que são afectadas ou responsáveis por elas, tendo como resultado a integração de toda a organização no processo de gestão de risco operacional (Mestchian 2003). Permite também a disponibilização de avisos prévios, que servem como indicadores para o controlo e uma efectiva gestão estratégica de risco operacional.

Tanto em *scorecards*, quanto noutros relatórios, os KRI's (*Key Risk Indicators*) têm sido das métricas mais utilizadas. Estas medidas são identificadas na fase de levantamento de requisitos e devem, tanto quanto possível, representar indicadores críticos que ajudem a gestão a identificar e controlar as principais fontes de risco operacional dentro da organização (Blunden 2003). Estes indicadores devem ser comparáveis com valores de referência externos e permitir a combinação de medidas quantitativas e qualitativas.

Enquanto área relativamente recente, ainda não existem tendências muito fortes sobre o tipo de relatórios a produzir no âmbito da gestão de risco operacional (a

excepção são os relatórios exigidos pelo supervisor, de acordo com a opção de abordagem regulamentar feita pela instituição). No entanto, sendo uma das principais responsabilidades dos gestores de risco o desenho e a disseminação de relatórios de risco operacional pelos diferentes órgãos da estrutura da organização, existem já alguns relatórios que se encontram presentes na maioria das implementações de sistemas de informação. Destes, destacam-se o top 10 dos riscos operacionais; o cálculo das perdas esperadas e não esperadas; os piores casos de perdas durante determinado período temporal; os resultados de análises de stress, valores e limites de indicadores-chave de risco; a análise a fontes de dados externas (como, por exemplo, taxas de referência de perdas da indústria); o impacto das medidas de mitigação; a frequência e impacto de perdas por unidade de negócio, departamento, região, país entre outras dimensões; a análise de eventos, incluindo causas, controlos falhados e alocação a linhas de negócio; os mapas de risco; os custos e benefícios de medidas de mitigação e de opções estratégicas de investimento; o capital em risco e um reporte integrador (*Dashboards)* que permita à gestão ter um resumo de todas as actividades e áreas da gestão de risco operacional, de forma a garantir que a instituição está dentro dos limites estabelecidos na sua estratégia e, em caso de necessidade, tomar as medidas adequadas para regularizar qualquer situação que se encontre fora dos limites definidos. Outro conjunto de relatórios que têm conquistado crescente importância nas instituições financeiras, que não têm vindo, em contraste, a receber destaque nos diferentes estudos e bibliografia existente, são os relatórios de acompanhamento dos processos internos de risco operacional, ou seja, referentes a informação sobre os níveis de assimilação dos conceitos e importância do risco operacional por parte dos diferentes níveis da instituição. O número de acessos por utilizador, a duração entre a descoberta de um evento e o seu registo, o tempo de resposta a questionários, a qualidade e o detalhe da

informação introduzida no sistema, o número de medidas de mitigação desenvolvidas e a capacidade de resposta das unidades à sua implementação são alguns exemplos de relatórios de suma importância para os órgãos de gestão de risco operacional, pois facultam uma visão de como a instituição entende o risco operacional, permitindo, se necessário, implementar planos de mitigação para ajustar o comportamento diário da instituição aos objectivos do seu programa de gestão de risco operacional.

Uma tendência crescente a salientar é a necessidade de agregar informação de diversas áreas da instituição (Risco Operacional, Auditoria Interna, *Compliance*) dentro das mesmas análises e/ou relatórios. Este facto deve-se a estas três áreas partilharem muita da mesma informação-base (catálogos de riscos, controlos, processos) e contribuírem, todas elas, com dados para alguns dos relatórios internos e para os supervisores. Tendo por base este objectivo, alguns sistemas de informação vêm implementando estruturas de dados que lhes permitem interligar dados e as análises produzidas por cada uma destas áreas, de forma a construir uma "visão 360" sobre as diferentes dimensões de análise do sistema. Por exemplo, é possível desenvolver um relatório de *compliance* que apresente um processo e as suas actividades, com os diferentes riscos a elas associadas e os controlos que mitigam cada um destes riscos. Deste relatório, farão também parte os eventos de risco operacional detectados para estas actividades e os resultados das auto-avaliações realizadas a cada um dos riscos. Da auditoria interna, virão dados referentes aos testes realizados aos controlos, bem como às medidas de mitigação implementadas para corrigir deficiências detectadas.

Sejam ou não implementados sistemas de informação sofisticados, as melhores instituições irão desenvolver e fornecer aos gestores seniores informação sobre o risco operacional e a sua gestão. Esta informação pode variar entre a exibição de listagens de dados e relatórios bastante complexos. No dia-a-dia, a gestão ao nível da linha de

negócio pode servir-se de sistemas de informação de gestão de risco operacional para mais facilmente visualizar avaliações de risco, localizar indicadores de risco, concentrações de classes de risco e análises a planos de mitigação. Munidos destes dados, os gestores podem monitorizar mais eficazmente as suas actividades, reduzir perdas e melhorar o seu negócio através de uma maior optimização dos seus recursos, de forma a garantir melhores resultados e uma alocação óptima de capital para risco operacional.

3.4 – Linhas orientadoras para os futuros sistemas de informação para gestão de Risco Operacional

Com a implementação do Acordo Basileia II começou o desenvolvimento substancial dos sistemas de informação para a gestão de risco operacional, e foi com base nos requisitos deste Acordo que foram definidas as funcionalidades existentes nestes sistemas de informação. Dependendo do nível de sofisticação de cada instituição financeira ou da abordagem regulamentar que cada uma pretendesse implementar, as funcionalidades destes sistemas centravam-se sempre na construção da base de dados de risco operacional, no desenvolvimento de modelos analíticos e na estruturação de relatórios de gestão e para o supervisor. No entanto, desde o início deste desenvolvimento que foram detectadas algumas fragilidades (ou desafios) para os quais estes sistemas necessitam dar resposta. Netter e Poulsen (2003) identificaram um conjunto de desafios associados à tipologia de dados, que exigem dos futuros sistemas de informação uma solução robusta. O primeiro destes reptos coincidiu com a dificuldade em transformar informação qualitativa em equações quantitativas. Muitas das implementações de sistemas de risco operacional concentram-se em dados de

eventos de perda e questionários normalmente compostos por questões qualitativas. Ter a capacidade de transformar estes dados qualitativos em dados passíveis de modelar de forma a utilizar no processo de gestão tem-se revelado, segundo estes autores, outro dos grandes desafios, devido a questões como a clareza e entendimento das questões colocadas, as escalas de resposta empreendidas e a interpretação dos resultados obtidos. Outro repto identificado assenta no facto de a informação quantitativa de que o sistema necessita poder não estar correcta ou completa. Este ponto já foi referenciado em capítulos anteriores, e torna-se mais relevante devido à escassez de dados quantitativos para a análise de risco operacional. Seja por razões culturais, que dificultam o reporte de eventos de perda, seja pela dificuldade em consolidar toda a informação relativa a esses mesmos eventos, muitas bases de dados sofrem de falta de massa crítica e de qualidade de dados para análises robustas. Os futuros sistemas de informação deverão incorporar funcionalidades que não só incentivem, como apoiem as instituições a recolher informação de dados de eventos de perdas, com todo o conjunto de informação necessária para o seu programa de gestão de risco operacional. Por último, os supracitados autores detectaram o desafio que emerge da indispensabilidade de analisar diferentes fontes ou causas de risco. Os sistemas de informação hoje implementados não possuem grandes capacidades de diferenciar as suas análises de acordo com o tipo de risco operacional (e.g. fraude, falhas de sistemas, erros humanos). A diversidade de riscos que os sistemas de gestão de risco operacional têm de abarcar é enorme, com cada um destes riscos a apresentar uma especificidade tanto nos dados que o caracterizam, quanto no seu comportamento e nas suas consequências. Esta variedade torna virtualmente impossível a aplicação do mesmo conjunto de análises a todos estes riscos, o que vai implicar que, no futuro, os sistemas de informação sejam chamados a incluir estratégias de análise específicas para cada um dos riscos que têm de gerir.

Kingsley et al. (1998) centram as suas afirmações sobretudo em aspectos de supervisão e de transparência para os quais os sistemas de informação devem garantir uma resposta, tais como: (i) a existência de uma ligação à base de dados com a informação dos eventos registados e dos diferentes modelos aprovados para utilização nas análises; (ii) a presença de métodos de seguimento do processo de gestão de risco operacional, de forma a tornar as análises transparentes a auditorias internas e ao supervisor; (iii) a capacidade de acesso ao sistema para possibilitar anexar explicações e informação comparativa, que suportem as decisões tomadas como, por exemplo, as decisões referentes a medidas de mitigação; e (iv) a funcionalidade para a construção de relatórios visando a apresentação e comunicação da informação, que será o ponto central de contacto entre a área de gestão de risco operacional e a instituição, o supervisor e o mercado.

Para responder a estes desafios, Netter e Poulsen (2003) propuseram uma arquitectura de sistema de informação para gestão de risco operacional que permite estabelecer actividades que potencia a recolha de dados de risco operacional, a sua análise e a disponibilização de toda a informação necessária para a gestão dos riscos identificados. Esta arquitectura deve conduzir igualmente análises quantitativas e qualitativas circunscritas (por tipo de risco), ganhando perspicácia sobre a exposição ao risco operacional da instituição e sobre a sua resposta (mitigação) para a concretização dos objectivos definidos no seu programa de risco operacional. Por fim, deve ter a capacidade de reportar o perfil de risco operacional da instituição à gestão executiva, garantindo que esta dispõe de toda a informação para o integrar na sua estratégia global.

Também Chorafas (2001) identificou algumas das características base que as futuras evoluções dos sistemas de informação para risco operacional devem incluir, nomeadamente: (i) necessidade de controlo, gestão e resposta em tempo real por parte

do sistema de informação – para que os diferentes órgãos de gestão possam incluir nas suas decisões diárias dados de risco operacional; (ii) capacidade para tratar e analisar situações de baixa frequência e impacto elevado – o risco operacional é, em grande parte, a análise de eventos extremos, para os quais não há informação prévia; (iii) garantir respostas fiáveis em relação a sistemas de difícil compreensão – como já foi apresentado, a gestão de risco operacional é a gestão de eventos que envolvem factores humanos, com características que dificultam a sua modelação. É necessário que a próxima geração de sistemas de informação permita disponibilizar análises e indicadores que possibilitem gerir este tipo de eventos.

Hoffman (2002) apontou três elementos principais fundamentais ao futuro desenho e desenvolvimento de sistemas de informação para gestão de risco operacional. Estes sistemas deverão ser integrados nos sistemas globais de planeamento e estratégia da organização, por forma a criar-se um sistema integrado de partilha de informação, garantindo, assim, uma linguagem comum e transversal a toda a instituição, bem como análises que compreendam todos os dados necessários à obtenção das decisões mais acertadas. O primeiro destes elementos equivale à gestão e agregação de dados. O desenvolvimento de capacidades para a agregação de toda a informação de risco operacional numa base de dados central irá facultar a avaliação de múltiplas dimensões deste risco, permitindo um ilimitado número de análises, desde a análise de cenários à projecção sobre exposições futuras, passando pela correlação e análises de sensibilidade, pela análise causal, entre outras. Segundo este autor, estas bases de dados devem possuir duas características fundamentais: ser abertas, no sentido em que possibilitem aceder e ser acedidas por outros sistemas, e dinâmicas, para que possam acomodar a integração de novas fontes de informação que apresentam estruturas de dados diferentes da actual. O segundo elemento refere-se à análise de risco e sua

medição. Aqui, é identificada a necessidade da aplicação de modelos a eventos e factores de risco que se possam ajustar aos dados da instituição, cujos resultados vão ser utilizados para cálculos regulamentares e para a tomada de decisão relativa a níveis de risco da instituição e a medidas de mitigação a aplicar. O terceiro elemento é a capacidade de reporte do sistema, que deve permitir transformar, de forma rápida e dinâmica, os dados armazenados em informação, facultando aos decisores da instituição reagir às mudanças do ambiente, identificar novas direcções estratégicas e descobrir fontes de risco potencial antes que este se materialize. Associado a este elemento está também o conceito de metadata (informação sobre os dados), que irá outorgar aos utilizadores uma compreensão mais plena acerca de determinados atributos dos dados ou das metodologias utilizadas para a agregação dos dados e cálculos realizados. De acordo, ainda, com Hoffman (2002), existem outras capacidades que podem ganhar importância em sistemas mais abrangentes de risco operacional, tais como: (i) a ligação com outros sistemas existentes na instituição para a troca de informação, seja esta troca feita em tempo real seja em *batch*; (ii) dependendo da sofisticação da metodologia de gestão de cada instituição, pode revelar-se necessária a capacidade de análise e reporte em tempo real para a integração desta informação nas decisões mais operacionais da instituição; (iii) para instituições de maior dimensão e presentes em diferentes localizações geográficas, tornar-se-á importante que o sistema de informação tenha fortes níveis de escalabilidade e possa suportar conceitos de muti-língua e multi-moeda; (iv) questões de segurança e auditoria são aspectos críticos devido ao nível elevado de sensibilidade que normalmente está presente nos dados destes sistemas, o que faz com que o seu acesso deva ser altamente controlado e monitorizado. Quanto às funcionalidades de auditabilidade do sistema, estas são requisitos do supervisor, no âmbito do pilar II do Acordo de Basileia II, e o garante, para entidades internas e

externas, de que a informação do sistema, análises e relatórios foram obtidos de forma transparente e de que as metodologias de gestão interna e as indicações do supervisor estão a ser correctamente aplicadas.

De todas as áreas em que os sistemas de informação para gestão de risco operacional precisam evoluir, as áreas da modelação de eventos, de factores de risco e impactos e da identificação e compreensão do comportamento das diversas entidades geradoras de risco operacional são aquelas que apresentam maiores desafios. Isto sublinha o papel-chave da previsão, utilizando modelos quantitativos e qualitativos, acrescidos de regras que descrevam comportamentos extremos do sistema e da análise pormenorizada dos seus próprios mecanismos. Em relação à complexidade do sistema que se pretende modelar, é lícito dizer-se que, quando este é simples, as equações numéricas podem, com um certo grau de certeza, reproduzir o seu comportamento. Para sistemas mais complexos, nos quais devemos considerar diferentes níveis de abstracção, poder-se-á recorrer a redes neuronais – que, relativamente a modelos mais tradicionais, não requerem hipóteses sobre a função a ser estimada, ou a "*fuzzy logic*" –, para analisar eventos cuja informação é subjectiva, incompleta ou pouco fiável (Cruz 2002). Apesar de outras ciências, como a química, ensinarem que, tratando-se de previsão de acontecimentos habituais, é quase sempre possível encontrar, no passado, uma situação muito idêntica que nos permite ter uma referência para efectuar previsões, na situação de risco operacional, bem como noutras que sucedem em instituições financeiras, esta antevisão pode ter de recorrer a diversos casos anteriores, sem que nenhum corresponda adequadamente à situação corrente. Este desafio tem vindo a ser enfrentado por sistemas de informação baseados em técnicas de *data mining*, que, socorrendo-se de análises de segmentos e associações ou padrões, conseguem fornecer um conjunto de informação mais rica sobre a realidade do risco com que a empresa depara, por

exemplo, sobre quais as causas que mais influenciam um determinado evento. Koyuncugil e Ozgulbas (2008) apresentaram uma metodologia utilizando algoritmos CHAID para árvores de decisão, que aplicam a dados de pequenas e médias empresas, para a identificação, nestas organizações, de indicadores de risco operacional. Outra área a que se poderá também recorrer é a inteligência artificial (Cruz 2002), onde técnicas como *fuzzy logic*, algoritmos genéticos, ou redes neuronais têm vindo a demonstrar elevada capacidade na modelação de situações reais – existem já diversas aplicações na área de risco de mercado, que poderão traduzir-se numa forte ajuda na área de risco operacional, pois apresentam modelos de dados, metodologias e análises que incluem conceitos de negócio comuns ao risco operacional, tais como os conceitos de distribuição de perdas ou de medidas de mitigação.

Outras duas áreas que ainda carecem de desenvolvimento, tanto a nível teórico quanto da sua implementação em sistemas de informação para risco operacional, correspondem à correlação entre diferentes riscos e à quantificação e perdas indirectas (Mestchian 2003). No primeiro caso, o problema centra-se em tentar perceber até que nível diferentes riscos estão correlacionados – um dos exemplos mais frequentes é a sólida ligação que existe entre falhas nos processos nas instituições financeiras (risco operacional) e riscos identificados como risco de crédito (erros na aprovação de créditos devido à má qualidade de dados) ou de mercado (erros na execução de transacções nas salas de mercado devido a falhas de sistemas). Verifica-se, ainda, uma dificuldade considerável em conseguir correlacionar e separar cada uma das fontes de risco e o seu peso em cada um dos eventos a que a instituição está sujeita (Medova 2002). No segundo caso, trata-se da capacidade de medir e compreender não só as implicações directas de determinado evento, mas também as implicações indirectas (e.g. risco de

reputação) – os sistemas de informação fundados em modelos de *Activity Based Management* poderão ser um primeiro passo.

Nesta investigação foi possível identificar um número significativo de instituições financeiras que já implementaram sistemas de informação para gestão de risco operacional, que têm tido como objectivo principal apoiar estas instituições na resposta aos requisitos do supervisor. O investimento necessário em meios humanos e tecnológicos faz com que os órgãos de gestão revejam estes sistemas como algo mais estruturante do que apenas como uma resposta aos objectivos da supervisão, tentando, com base neles, desenvolver uma cultura de gestão de risco operacional dentro das suas instituições. Contudo, o desenvolvimento da cultura de gestão de risco operacional e, consequentemente, de novas métricas e metodologias de gestão dentro das instituições vem exigir novos sistemas de informação, com funcionalidades renovadas, que suportem as diferentes necessidades e opções de gestão de cada instituição, incluindo as decisões referentes ao perfil de risco e às medidas de mitigação adoptadas. No presente, as instituições financeiras encontram-se numa fase crucial de escrutínio sobre qual deverá ser o papel dos sistemas de informação no seu processo de gestão de risco operacional. Sem dúvida que a evolução dos sistemas de informação estará claramente ligada a esta decisão e aos resultados que forem alcançados com a sua implementação, sendo que estes sistemas irão ter um impacto fundamental no sucesso dos programas de gestão de risco operacional de cada instituição.

III PARTE – INVESTIGAÇÃO

4 – METODOLOGIA

A escolha da metodologia a ser aplicada neste trabalho teve como objectivo responder ao desafio de apresentar um desenho funcional do que deverá ser um sistema de informação para a gestão de risco operacional em instituições financeiras, capaz de responder aos requisitos identificados pela revisão da literatura, mas também aos que constituem hoje os requisitos reconhecidos pelas instituições financeiras portuguesas e pelos seus supervisores. A informação foi recolhida através de questionários enviados às diferentes entidades; para o desenvolvimento do desenho funcional do sistema foi utilizada a *Soft System Methodology*.

A análise de sistemas consiste, basicamente, em raciocinar de uma maneira estruturada, prestando a devida atenção à dinâmica do sistema e, por vezes, aos processos não lineares e/ou estocásticos de interacções entre os recursos desse sistema (pessoas, materiais, componentes e informação), bem como ao ambiente em que opera (Reisman & Oral 2004).

Sempre que o objectivo passa por endereçar problemas de gestão, em que a análise de sistemas desempenha um papel fundamental, existem duas metodologias fundamentais às quais importa recorrer (Reisman & Oral 2004), a saber:

1. *Soft System Methodology* (SSM) – modelo conceptual;
2. *Hard System methodology* (HSM) – modelo formal.

4.1 – *Soft System Methodology*

A contribuição da SSM é valiosa, no sentido em que gere a identificação do problema de uma forma organizada. A SSM já foi articulada, estabelecida, validada e

legitimada de muitas formas (e.g. uma publicação de SSM foi eleita como “50th Anniversary [JORS] Paper”).

A complexidade do problema na análise de sistemas incorpora a intervenção humana, o que determina que os sistemas sejam abertos e dinâmicos. Consequentemente, estes reagem e mudam de forma constante, mesmo durante as primeiras fases de análise – é precisamente neste ponto que a SSM pode prestar um importante contributo, ao passo que a HSM é mais utilizada numa fase mais tardia na implementação do próprio sistema.

Uma das fases mais relevantes na análise e implementação de sistemas equivale à descrição do sistema. Sem qualquer dúvida, a SSM parece endereçar todas as questões desta etapa através de perguntas como (Reisman & Oral 2004):

1. Qual é o problema real?
2. Quais são os objectivos a atingir, tendo em conta a percepção da situação actual do problema?
3. Quais são os constrangimentos?
4. Quem são os intervenientes?
5. Quem são os beneficiários?
6. Quem são os reguladores?
7. Qual é o sistema e quais os ambientes envolvidos?
8. Como vai o sistema realizar as suas funções?
9. Quais os seus subsistemas?
10. Quais deverão ser os critérios de avaliação do sistema?

A SSM detém uma missão crucial na identificação / definição de um sistema, além de que se mostra capaz de apresentar a solução funcional para que, na fase seguinte,

possa ser utilizada a HSM, no que respeita à implementação prática dessa mesma solução (Reisman & Oral 2004). Sendo a definição de um sistema de informação para gestão de risco operacional um dos principais objectivos deste trabalho de investigação, a SSM reúne as características fundamentais para que fosse a metodologia aplicada.

4.2 – Processo de investigação

Actualmente, ainda existe um parco conhecimento sobre o estado de desenvolvimento dos sistemas de informação para gestão de risco operacional em instituições financeiras portuguesas. Não se verifica sequer a presença de informação estruturada sobre a abordagem à gestão de risco operacional de cada instituição, definindo, claramente, os seus objectivos. Tendo como meta recolher informação sobre estes dois vectores, foi desenvolvido um processo de investigação cuja finalidade cimeira passa por encontrar respostas para três questões fundamentais, nomeadamente:

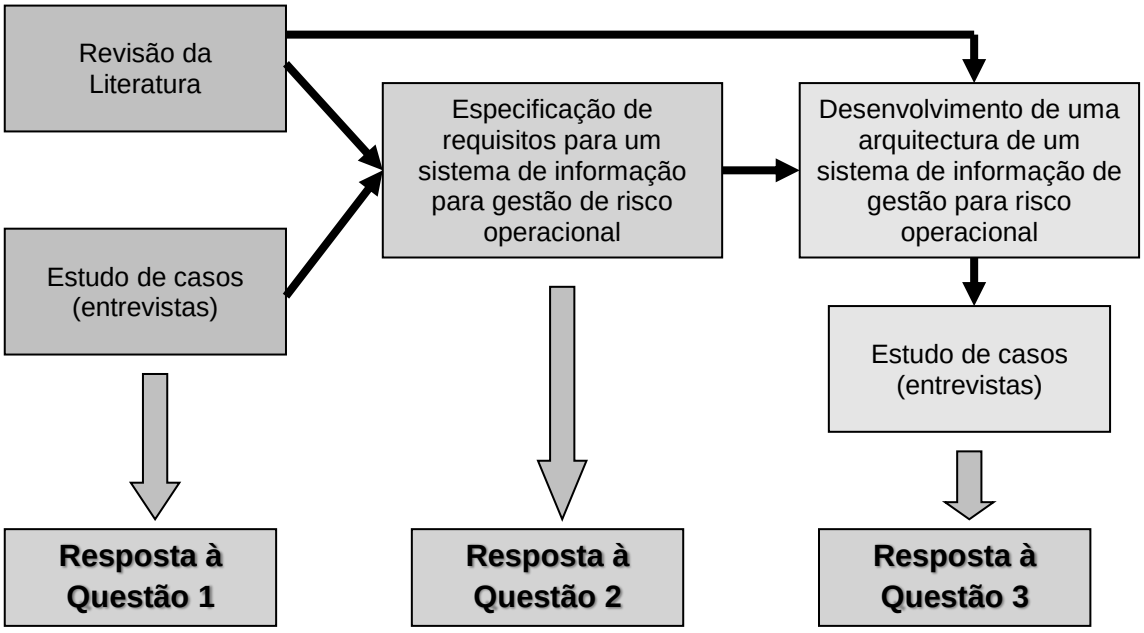
Questão 1: O risco operacional é reconhecido pelas instituições financeiras portuguesas enquanto tema que necessita de atenção?

Questão 2: Existe a possibilidade de especificar requisitos para um sistema de informação para risco operacional em instituições financeiras?

Questão 3: Há possibilidade de propor uma arquitectura adequada à gestão de risco operacional por parte das instituições financeiras portuguesas?

Objectivando o alcance deste propósito central, foi desenhado um processo de investigação que se apresenta na figura 8 – Processo de investigação.

Figura 8 – Processo de investigação



O processo de investigação apresentado assenta em três vectores principais: o primeiro visa a revisão da literatura existente – apesar de já haver investigação nesta área, esta ainda é segmentada por blocos (dados, análises, relatórios); a verdade é que só muito recentemente se começa a analisar o sistema de informação como um todo. O segundo refere-se à realização de entrevistas compostas por um conjunto de questões pré-definidas – estas questões foram o resultado da análise levada a cabo com base em entrevistas não estruturadas, efectuadas no ano de 2007. Todas as entrevistas foram conduzidas pelo autor deste trabalho e efectivadas de forma presencial ou através do envio das questões por correio electrónico. Não foi definida qualquer estrutura para as respostas por parte dos intervenientes – trata-se de uma área em que as especificidades dentro das organizações podem suscitar respostas bastante distintas (Sekaran 2003). A população-alvo destas entrevistas divide-se entre nove dos maiores bancos e sete seguradoras a operar em Portugal. Esta escolha baseou-se num estudo preliminar, realizado pelo autor (entrevistas não estruturadas), que revelou serem estas as

instituições com mais possibilidade de implementarem modelos de sistemas de informação para risco operacional mais avançados (não foram consideradas instituições cuja implementação de sistemas para gestão de risco operacional tenha a sua base fora do território português). No terceiro vector, irá ser aplicada a SSM, apresentada no capítulo anterior, para o desenho conceptual do sistema; neste, serão considerados os requisitos e as funcionalidades identificados nos dois vectores anteriores.

4.3 – O Risco Operacional nas instituições financeiras portuguesas

Um dos objectivos fundamentais desta tese é avaliar o entendimento que as instituições financeiras em Portugal possuem sobre o tópico do risco operacional, mais concretamente, sobre os sistemas de informação para gestão deste risco. Para tal, foi elaborado um questionário (em anexo) que foi enviado a um conjunto de instituições financeiras da área bancária e da área seguradora, assim como às entidades reguladoras de ambos os sectores.

O questionário enviado às instituições financeiras pretende revelar três aspectos fundamentais:

1. Qual a visão, e importância, dada à gestão de risco operacional dentro de cada umas destas instituições – factores que levam ao seu desenvolvimento, abrangência e objectivos;
2. Qual é a estrutura do sistema de informação que dá suporte a essa visão – funcionalidades, arquitectura;
3. Como é visto o futuro da gestão de risco operacional e quais os requisitos para o sistema de informação que a irá suportar – oportunidades, mais-valias, desafios e novas funcionalidades.

Na escolha da amostra, tentou-se seleccionar o número máximo de instituições financeiras para participarem no estudo – por diferentes razões, entre as quais se destacam a inexistência de programas sólidos de risco operacional, a dependência destes programas da estratégia do grupo com sede em países que não Portugal, ou a dificuldade em garantir a colaboração da instituição, levaram a amostra a centrar-se nas instituições que são apresentadas. No entanto, e para efeito de análise dos resultados, há que considerar os seguintes aspectos referentes à amostra utilizada no estudo:

1. Na selecção da amostra relativa ao sector bancário, foi utilizada, como métrica, o total de activos que cada instituição detém. Esta métrica tem a capacidade de representar o peso da instituição no mercado português, perfazendo, assim, um bom indicador do impacto de eventos de risco operacional neste sector. Utilizando como referência os valores apresentados pelo Banco de Portugal respeitantes ao ano de 2008, as instituições bancárias consideradas neste estudo englobam 83% do total de activos das instituições a operar em Portugal, o que, para efeitos de risco operacional, representa um valor de elevada significância sobre o nível de exposição do mercado bancário português a risco operacional.
2. Na escolha da amostra relativa ao sector segurador, foi usado, como métrica, o volume de prémios brutos que é facultado pelo Instituto de Seguros de Portugal (ano de 2008). Este valor permite ter uma noção do impacto que as seguradoras participantes no estudo imprimem no mercado português. O valor obtido foi de 40%, o que, apesar de ser um valor de alguma relevância, não permite, na opinião do autor, estabelecer conclusões com a solidez das estabelecidas para a banca. Infelizmente, à data do estudo

> não foi possível recolher a opinião de mais seguradores, facto que pode estar directamente relacionado com o atraso do Acordo Solvência II – esta deverá ser uma questão a ser abordada em futuros trabalhos de investigação.

Sempre que possível, foi recolhida informação de diferentes áreas dentro das instituições, incluindo os departamentos responsáveis pelo risco operacional, bem como das áreas de sistemas de informação. Devido à crescente expansão desta temática a outras funções operacionais no cerne das instituições, como os departamentos de Auditoria Interna e *Compliance*, é vital que, futuramente, a investigação se estenda também a estas áreas.

Com base nos critérios já referidos, e também de acordo com a disponibilidade obtida, foram as seguintes as instituições que deram o seu contributo para este estudo:

1. Companhia de Seguros Açoreana
2. Banco Banif
3. Banco BIG
4. Banco Espírito Santo
5. Banco BPI
6. Caixa Seguros
7. Caixa Geral de Depósitos
8. Companhia de Seguros Tranquilidade
9. Seguradora Eurovida
10. Finibanco
11. Seguradora Generalli
12. Banco Millenium BCP
13. Montepio Geral

14. Banco Santander Totta

Houve ainda mais duas instituições que contribuíram para o estudo, mas que, em respeito a normas internas, exigiram que o seu nome não fosse directamente apresentado no presente trabalho.

Da parte das entidades reguladoras, o contributo foi obtido através do Banco de Portugal (BP) e do Instituto de Seguros de Portugal (ISP). Nestes casos, o questionário pretende revelar os seguintes aspectos:

1. Como a entidade reguladora espera que as instituições financeiras venham a abordar a gestão de risco operacional;
2. Qual o papel que deverá ser representado por um sistema de informação neste âmbito.

Espera-se que as respostas obtidas permitam identificar um conjunto de características e necessidades que concorram para o desenvolvimento de sistemas de informação que potenciem uma melhoria dos processos de gestão de risco operacional e contribuam para a promoção de instituições mais eficientes e eficazes, capazes de garantir a sua sobrevivência e a solidez do sistema financeiro (principais objectivos das entidades reguladoras).

IV PARTE – RESULTADOS

5 – ANÁLISE AOS RESULTADOS OBTIDOS

Como referido anteriormente, as respostas aos questionários foram abertas para permitir uma maior amplitude nas opções e requisitos identificados por cada uma das instituições. Desta forma, o resultado não fica condicionado por uma visão pré-definida de gestão de risco operacional e de um sistema de informação para a acomodar, permitindo que cada instituição apresente as suas abordagens, objectivos, requisitos e desafios. Com base nas respostas de cada instituição, foram identificados, para cada questão, os elementos críticos para análise. As respostas obtidas foram trabalhadas individualmente. No entanto, a sua apresentação é feita de forma agregada, com o objectivo de assegurar a confidencialidade das respostas obtidas por parte de cada instituição (requisito essencial da maioria das instituições para participar neste estudo), sem que esta situação comprometa a fiabilidade das análises efectuadas.

5.1 – Resultados preliminares

Durante o ano de 2007, foi realizado um conjunto de entrevistas preliminares com directores de risco operacional e responsáveis da área de sistemas de informação de 10 instituições financeiras portuguesas (todas estas instituições integraram o estudo final). Estas entrevistas tiveram como objectivo fazer uma primeira avaliação do grau de maturidade destas instituições face ao conceito de gestão de risco operacional e à necessidade objectiva de sistemas de informação específicos para este tópico.

Deste primeiro conjunto de contactos realizados, foi possível retirar algumas conclusões preliminares sobre a visão que as instituições financeiras tinham da gestão de risco operacional e sobre o papel dos sistemas de informação. A primeira conclusão

que se tornou evidente foi que, apesar de Buchlet e Unteregger (2004) afirmarem que o risco operacional já era gerido antes do surgimento do Acordo Basileia II, o desenvolvimento recente da área da gestão de risco operacional nas instituições financeiras portuguesas alicerça-se fundamentalmente nas pressões regulamentares dos Acordos Basileia II e Solvência II. A maioria das instituições não dispunha de programas formais de gestão de risco operacional, recaindo na direcção de Auditoria Interna algumas das funções a que hoje se chama gestão de risco operacional (e.g. identificação de eventos e planos de mitigação). No entanto, as novas pressões regulamentares têm persuadido as instituições para equacionar a implementação de sistemas de gestão de risco operacional, essencialmente com o objectivo de responderem aos requisitos do documento "*Sound Pratices for the Management and Supervision of Operational Risk*". A decisão estratégica sobre a abordagem que cada instituição pretende adoptar para a gestão de risco operacional tem exercido impacto sobre os níveis de celeridade e abrangência dessas implementações. Ficou também claro o facto de que estas instituições quererem, na sua maioria, aproveitar a implementação destes sistemas para criar métricas e processos de gestão de risco operacional mais avançados do que aqueles que detêm presentemente. Assim, o investimento que terão de fazer no sistema de informação para responder ao supervisor será valorizado, ao permitir atingir objectivos como os propostos por Kingsley et al. (1998), que envolvem eixos fundamentais para a instituição, como a redução de custos e garantir um crescente conhecimento das ameaças a que está interna e externamente exposta.

Salvo uma excepção, as diferentes instituições financeiras têm como principal prioridade a aquisição e o tratamento dos dados que irão suportar todo o sistema de decisão, construindo assim uma estrutura que suporte os objectivos apresentados por Mestchian (2003) e remetendo, para uma segunda fase, o desenvolvimento dos modelos

analíticos de decisão. Este aspecto releva duas preocupações constantes, associadas à implementação de sistemas de informação para risco operacional: (i) a elevada dificuldade presente na recolha dos dados necessários para suportar modelos analíticos fiáveis e apoiar na tomada de decisão – este ponto tem sido revelado por diferentes estudos referidos nesta investigação e por projectos de implementação em instituições distintas – e (ii) o facto de existirem ainda sérias dúvidas sobre o que deverá ser um sistema de informação para a gestão de risco operacional – as aplicações existentes no mercado são vistas como soluções ao encontro da regulamentação das entidades supervisoras e mostram-se pouco flexíveis e abrangentes para conseguirem responder aos requisitos de um programa integrado e global de gestão de risco operacional.

Como resultado deste primeiro conjunto de entrevistas, pôde-se também concluir que todas as instituições financeiras passaram a implementar a gestão de risco operacional com um processo com existência própria e não integrada noutras direcções, tendo a sua própria estrutura e objectivos integrados na estratégia global da instituição. Para apoiar este novo processo, identificaram a necessidade de sistemas de informação para a gestão de risco operacional (apesar de com diferentes níveis de sofisticação), que, numa primeira fase, deverão ter como principal objectivo responder às disposições legais das entidades supervisoras. Apesar de a sua difusão ter estado associada a pressões regulamentares, todas as instituições reconheciam a importância e abrangência que a gestão de risco operacional representará para um melhor funcionamento das suas organizações; reviam, pois, os sistemas de informação como um dos pilares axiais de um processo de gestão de risco operacional mais evoluído, capaz de desenvolver competências e criar valor dentro da instituição.

5.2 – Resultados dos questionários

Os resultados obtidos serão distribuídos por dois capítulos principais: um representativo das instituições bancárias; o outro referente às instituições seguradoras. Esta divisão deve-se a duas questões fundamentais: a primeira, inerente às diferenças existentes entre as duas actividades de negócio; a segunda prende-se com o nível dos requisitos exigidos pelos reguladores e com o estado de maturidade da gestão de risco operacional nas instituições estudadas. Um terceiro capítulo será dedicado à interpretação das respostas fornecidas pelas entidades supervisoras. No contexto de cada capítulo, apresentam-se os resultados agregados para cada uma das perguntas do questionário (em anexo). No final, é exposto um resumo das conclusões obtidas a partir da análise das respostas das diferentes instituições e supervisores. Juntamente com a revisão da literatura, este estudo completará a base para o desenho funcional de um sistema de informação para gestão de risco operacional mais amplo e apto para responder aos desafios colocados por reguladores e mercado em geral.

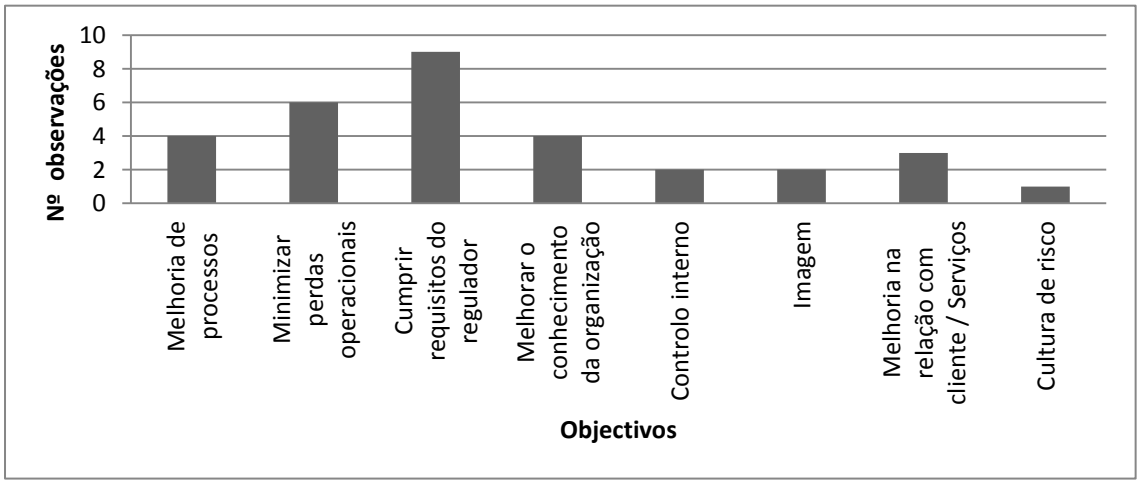
5.2.1 – Instituições Bancárias

Como nota introdutória, convém salientar que as instituições bancárias revelaram uma elevada capacidade em interpretar as questões colocadas neste estudo, no que concerne os desafios da gestão de risco operacional nas suas organizações e o papel de um sistema de informação para suportar esta gestão.

Na primeira questão, pedia-se que os bancos enunciassem os objectivos (Figura 9 – Objectivos da gestão de risco operacional na banca) que os motivaram a implementar procedimentos para a gestão de risco operacional. A finalidade que mais se destaca é a

necessidade de cumprir com os requisitos da entidade supervisora; propósito, esse, não considerado pela literatura inicial, que colocava a tónica em objectivos de gestão interna e performance (Kingsley, et al. 1998). Na realidade, antes do Acordo Basileia II, a área de risco operacional era tida como secundária, não se verificando, para a maioria dos casos, procedimentos estabelecidos ou áreas internas para tratar esta área. Na banca, o Acordo Basileia II representa, claramente, o factor impulsionador, que impele os bancos portugueses a criar departamentos e a implementar procedimentos e sistemas de informação para risco operacional. Alguns bancos rentabilizam os investimentos necessários para responder aos requisitos regulamentares, ao utilizar a gestão de risco operacional com o objectivo de melhorar os seus processos, minimizar as suas perdas operacionais, ou conseguir incrementar o conhecimento sobre as suas organizações. Entre os propósitos definidos, um número reduzido das organizações questionadas apontou o controlo interno (actividade dantes realizada pela direcção de Auditoria Interna), a melhoria da imagem, a cultura de risco da organização e a tentativa de melhorar tanto a relação com os clientes, quanto a qualidade dos serviços oferecidos. Ora, tudo isto anuncia o desenvolvimento de uma visão que engloba a gestão de risco operacional em processos mais globais da instituição, que não a revê somente como uma actividade em conformidade com os requisitos do supervisor, o que, de resto, vai ao encontro da definição apresentada por Vinella e Jin (2005) – que vêem no risco operacional um factor susceptível de influenciar tanto as perdas, quanto os proveitos da instituição – e da metodologia de gestão de risco operacional proposta por Dickstein e Flast (2009) – que interliga a gestão de risco operacional com os processos operacionais das instituições. Importa realçar que é esta a metodologia que a maioria das instituições analisadas tem vindo a aplicar na sua actividade de gestão de risco operacional.

Figura 9 – Objectivos da gestão de risco operacional na banca



A abordagem regulamentar à qual a maioria dos bancos portugueses se está a candidatar para risco operacional é a do indicador básico – apenas três das instituições consultadas referiram a abordagem *standard*, numa primeira fase. Esta circunstância deve-se em muito à dificuldade considerável que a maioria das instituições sentiu em definir internamente a forma como abordar esta nova temática, bem como a alguma incredulidade quanto às reais capacidades de poupança de capital conseguida com a aplicação de abordagens mais avançadas. Neste momento, os bancos já percorreram, contudo, um longo caminho e expandiram conhecimentos sobre requisitos, necessidades, desafios e oportunidades da gestão de risco operacional. Assim, é de esperar que, no futuro, a maioria das instituições progrida para as abordagens mais avançadas, apesar de até a data não haver dados que sustentem esta afirmação. Aliados a estes factores, existem pressupostos de imagem impostos pelo mercado e requisitos de empresas de *rating*, que têm direccionado os bancos para a implementação de procedimentos e sistemas os quais perfazem requisitos de abordagens mais exigentes – como foi apresentado no capítulo "Relatórios", existem vantagens competitivas para as instituições que consigam demonstrar a todo o sistema financeiro as suas capacidades

para gestão de risco operacional. Mas mesmo actualmente, ainda representam uma minoria as instituições que pensam avançar para a abordagem AMA – as críticas a esta abordagem, tais como as dirigidas por Moosa (2008), as questões colocadas por Kalhoff e Hass (2004) e Currie (2004) relativas à modelação de risco operacional e as dúvidas referentes aos reais benefícios a atingir com esta abordagem e custos associados à sua implementação, tudo isto fundamenta as principais razões para esta decisão.

As empresas foram questionadas em relação à forma como se encontram estruturadas para abordarem o tema do risco operacional. Na sua maioria, os diferentes bancos criaram departamentos para a gestão de risco operacional, ou colocaram a sua gestão dentro de departamentos de controlo interno. A minoria corresponde às empresas que alocaram recursos da sua direcção global de risco para a gestão de risco operacional ou que criaram direcções conjuntas entre o risco e o controlo interno. Esta decisão pode fundar-se na forma e objectivos da abordagem para risco operacional que as instituições decidiram seguir. Aquelas que, numa primeira fase, optaram por se concentrar prioritariamente na resposta aos requisitos regulamentares, colocaram as questões relacionadas com a gestão de risco operacional sob a esfera da direcção de risco, que já engloba o risco de mercado e o de crédito e onde já existe experiência e meios passíveis de responder a este novo desafio do supervisor. No caso de instituições com metodologias mais profundas para a gestão de risco operacional, a decisão sobre onde colocar este tópico centrou-se em direcções de controlo interno, nas quais o risco operacional pode ser integrado nas actividades de acompanhamento dos diferentes processos de negócio da instituição, podendo, assim, ser compreendido, analisado e mitigado dentro da estratégia global, tornando-se um pilar estruturante no funcionamento da instituição (Instituto de Actuários do Canadá 2010).

Em relação à estratégia que os bancos seguem para a recolha de informação para gestão de risco operacional, a quase totalidade dos bancos optou por uma estratégia descentralizada, em que, nas primeiras fases do processo de risco operacional, a informação é recolhida e tratada por entidades exteriores à própria direcção de risco operacional – pretende-se, assim, corrigir o problema relacionado com o possível desfasamento entre frequência e severidade apresentado por de Fontnouvelle (2006) e Allen e Bali (2004), bem como garantir o princípio vital de segregação de funções imposto pelo supervisor. No entanto, quando se aprofunda esta questão, encontram-se muitas instituições em que, apesar de usarem estruturas mais descentralizadas, na prática, a dificuldade na recolha de dados – associada, por vezes, ao problema da confidencialidade dos eventos (Haas & Kaiser 2004) e à ausência de uma cultura de risco que incentive a recolha desses eventos e a participação activa no processo de gestão de risco operacional – as força a recorrer a métodos mais centralizados, nos quais a direcção de risco operacional é chamada a recolher, ou a completar, muita da informação em falta por parte das outras direcções.

Uma situação reveladora desta problemática surge no procedimento de registo de recuperações associadas a eventos. Num elevado número de casos, a recuperação é realizada em períodos temporais distantes do evento e por uma direcção diferente – ou seja, não coincidente com aquela onde o evento ocorreu e/ou que o registou –, que não dispõe, por isso, do conhecimento necessário para que possa associar a recuperação a um determinado evento de risco. Este facto leva a que, em muitas situações, o registo das recuperações, ou da sua ligação ao evento, se traduza num procedimento executado de forma central pela direcção de risco operacional.

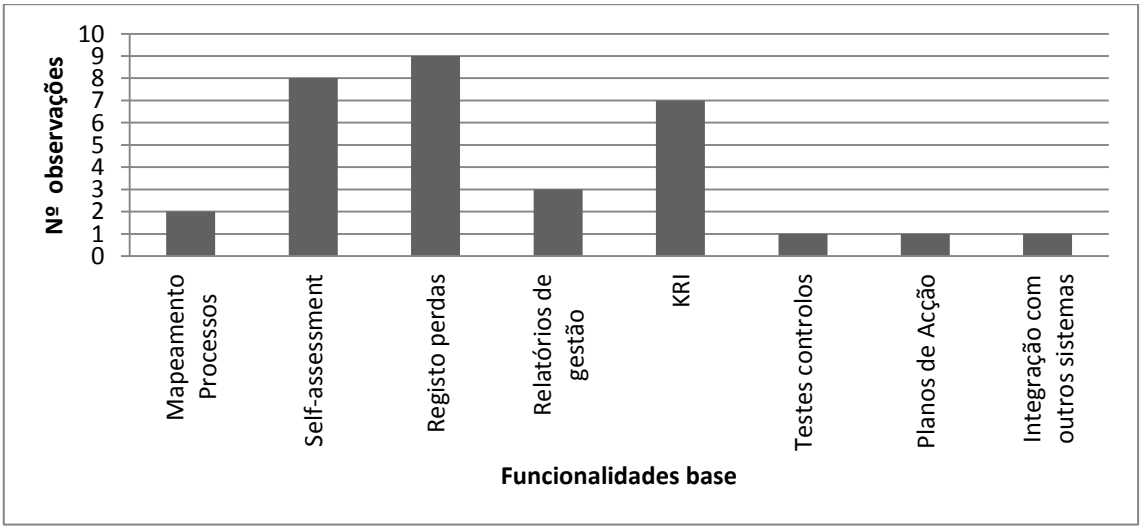
Quanto à questão referente à existência de um sistema de informação para a gestão de risco operacional, a resposta revelou-se unânime: todos os bancos consultados têm

implementado um sistema de informação para os apoiar no tópico do risco operacional. Sem dúvida que a pressão do supervisor para que as instituições financeiras tenham sistemas para a recolha e análise de eventos e factores de risco foi o principal catalisador para estas implementações. No entanto, o nível de sofisticação existente em alguns dos sistemas, ou os requisitos futuros identificados, demonstram já um estado de consciência avançado sobre a indispensabilidade de abordar o tema de gestão de risco operacional de forma mais objectiva e sustentada, assim como acerca da necessidade de um sistema de informação que, tal como Kross (2009) o preconizou, apoie no desenvolvimento de uma iniciativa corporativa de gestão de risco operacional.

As funcionalidades existentes nos sistemas de gestão de risco operacional (Figura 10 – Funcionalidades base nos sistemas de informação para risco operacional na banca) mais referidas pelos bancos foram: o registo de perdas, as auto-avaliações (*self-assessments*) e os indicadores de gestão de risco operacional (KRI's). Este resultado deve-se ao facto de, tanto nos documentos do Comité de Basileia (Basileia II, 2003), como na maioria da literatura existente (Mestchian, 2003), serem estes três os métodos mais apontados como fonte para a recolha de dados – por exemplo, a análise de cenários tem sido nitidamente uma área de mais fraca exploração por parte das instituições portuguesas. Apesar de estas serem as três mais implementadas nos sistemas de informação, existem bancos que requerem outro tipo de funcionalidades, de acordo com os objectivos que guiam a gestão de risco operacional. Funcionalidades como testes aos controlos, planos de acção e mitigação, relatórios de gestão, ou o mapeamento de processos, são requeridas não por requisitos regulamentares, mas pela necessidade de integração dos dados e análises da direcção de risco operacional com os das áreas de Auditoria Interna ou do *Compliance*, de forma a potenciar sinergias que permitam desenvolver uma melhor e mais eficiente gestão do risco operacional dentro das

organizações. A funcionalidade "integração com outros sistemas" alicerça-se na necessidade de recolher eventos, de outro modo difíceis de compilar, e na possibilidade de verificar a integridade e a validade da informação recolhida anteriormente. Neste ponto, encontra-se o tópico relevante da reconciliação contabilística, devido a esta ser uma fonte de eventos internos passível de utilizar para alimentar a base de dados de risco operacional, ou como meio de validação da informação nela armazenada, que tem sido reconhecida pelas instituições como uma funcionalidade que carece de ser desenvolvida. A complexidade deste desenvolvimento tem estado associada a circunstâncias aliadas à integração de sistemas em plataformas tecnológicas diferentes, mas a principal razão que vem impedindo a sua implementação centra-se nas diferenças existentes entre a metodologia de classificação e a estrutura de registo de eventos que a Contabilidade e o Risco Operacional têm utilizado – será necessário criar uma harmonização de regras para o registo das duas áreas, ou um mapeamento das classificações de forma a possibilitar uma integração benéfica para ambas.

Figura 10 - Funcionalidades base dos sistemas de informação para risco operacional na banca

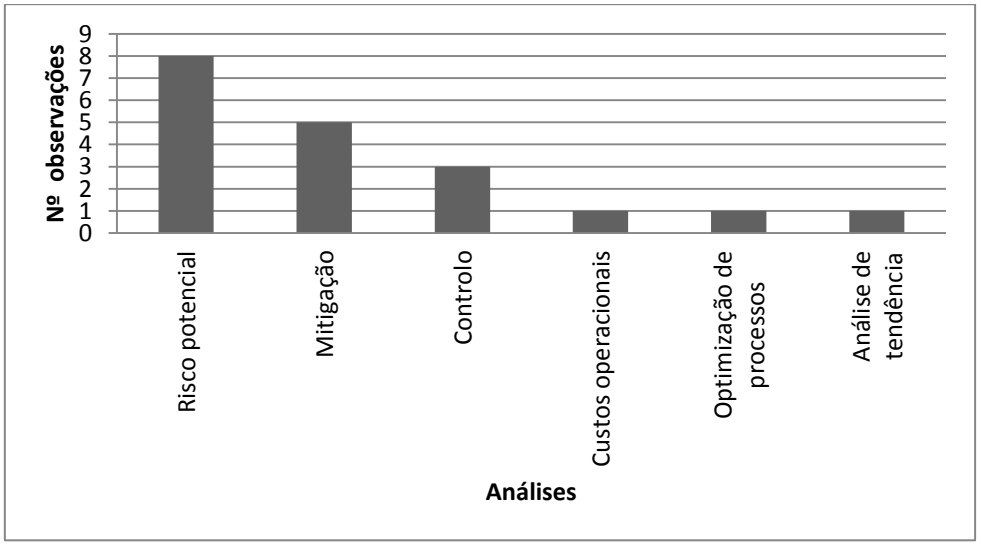


Na recolha de dados para alimentar os sistemas de informação existentes, a maioria dos bancos recorre ao carregamento manual da informação através de aplicações Web que facilitam um processamento descentralizado. Este facto deve-se, na prática, a duas razões fundamentais: (i) à existência diminuta de dados sobre risco operacional armazenados em suporte electrónico – não existia uma cultura nas instituições que fomentasse a recolha estruturada de eventos de risco operacional – e (ii) à dificuldade na categorização da informação já armazenada – inconvenientes já identificados por diversos autores, incluindo Muzzy (2003). Existem instituições que possuem preocupações crescentes com o carregamento manual e que têm vindo a tentar criar mecanismos semiautomáticos que permitam facilitar essa recolha por parte das linhas de negócio, seja através de carregamento via ficheiros EXCEL, seja por meio da funcionalidade de preenchimento automático de alguns dos dados. É, no entanto, de salientar que já existem bancos que vêm desenvolvendo a capacidade de recolher dados de forma automática dos seus sistemas operacionais (e.g. sistema de reclamações, Help Desk). Nestes casos, os problemas têm-se colocado na classificação e validade desta informação para que responda aos requisitos da gestão de risco operacional.

Quando confrontados com a questão sobre quais as análises que os seus sistemas de informação (Figura 11 – Análises requeridas na banca) deveriam facultar, os bancos apresentaram um conjunto diversificado de respostas. No entanto, duas análises se destacaram: o risco potencial a que os bancos estão, ou estarão, expostos e a análise do potencial das medidas de mitigação. Estas análises estão alinhadas com um dos objectivos para um sistema de informação apresentados por autores como Gibson (1997), Mestchian (2003) e Kross (2009), que indicaram a identificação de risco potencial como uma das principais razões que deveriam estar na base da implementação

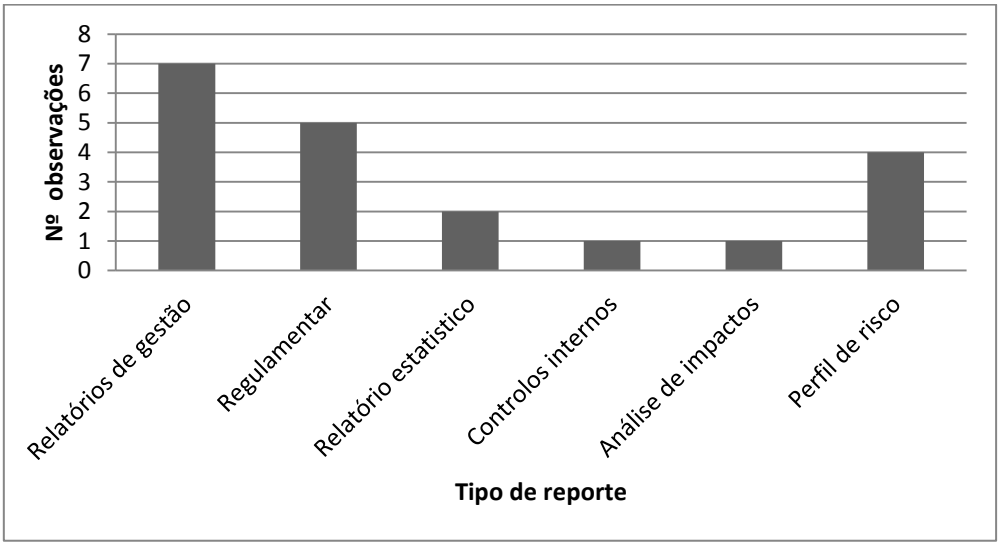
destes sistemas. Directamente associada a esta análise, está a avaliação das medidas de mitigação. Tendo em vista uma abordagem racional à gestão de risco operacional, as instituições querem realizar análises sobre o real impacto das suas medidas de mitigação na frequência e/ou severidade dos diferentes riscos, numa óptica de custo/ benefício que garanta o sucesso da sua estratégia dentro dos limites de risco e de custos estabelecidos. Outras análises identificadas por alguns bancos foram o controlo interno, os custos operacionais e a optimização de processos, bem como análises mais direccionadas para objectivos de melhoria operacional da instituição que lhes possibilitem garantir um serviço de maior qualidade aos seus clientes e melhores condições de trabalho aos seus colaboradores – elementos estruturantes para assegurar a rentabilidade e o sucesso da instituição. Um pormenor relevante a destacar prende-se com a ausência de menção a análises associadas a abordagens avançadas (e.g. AMA) – mais um indicador de que as abordagens avançadas de Basileia II não correspondem a um dos objectivos que as instituições financeiras considerem para os seus programas de gestão do risco operacional nos próximos anos.

Figura 11 – Análises requeridas na banca



Quanto ao reporte (Figura 12 – Reporte requerido na banca) que os bancos pretendem que lhes seja fornecido pelos seus sistemas de informação, destacam-se três tipos: em primeiro lugar, os relatórios de gestão e os de perfil de risco – ambos bons indicadores da relevância conferida à gestão de risco operacional por parte da gestão de topo dos bancos, que a vêem como uma fonte para melhorarem os seus níveis de eficiência interna e, consequentemente, reduzirem os seus riscos operacionais. Esta visão de reporte interno está mais orientada com o que é defendido por Blunden (2003) do que com as ideias de Watts e Zimmerman (1986) e de Helbok e Wagner (2006), que advogam um reporte externo que evite atenção não desejada por parte do supervisor e que potencie a imagem da instituição no mercado. O terceiro tipo de relatório mais pretendido é o regulamentar, que perfaz uma imposição fundamental do supervisor ao abrigo do pilar III do Acordo Basileia II, para o qual as instituições vão requerer o máximo de automatismo de forma a não sobrecarregar as suas direcções com esta actividade. Convém realçar que muitos dos reportes regulamentares não são produzidos só pela área de risco operacional, mas também pela de *Compliance*, além de que assentam em informação partilhada por ambas as áreas, o que implica um maior nível de atenção aos conceitos de negócio aplicados na base de dados e à forma como os reportes são estruturados.

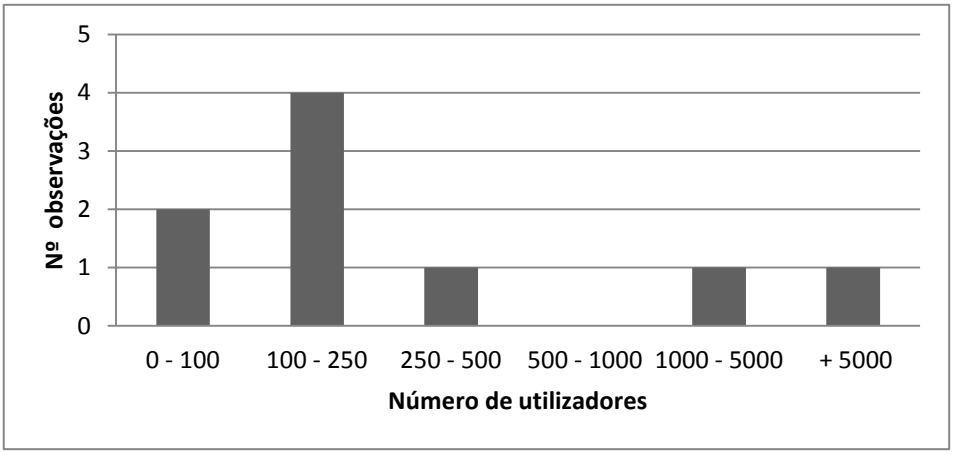
Figura 12 – Reporte requerido na banca



O número de utilizadores que cada banco tem a interagir com o seu sistema de informação para risco operacional (Figura 13 – Utilizadores do sistema de informação de risco operacional na banca) é bastante distinto de instituição para instituição – desde instituições com grupos de entre 0 e 100 utilizadores, até outras com mais de 5000 utilizadores. Tal circunstância poderia estar relacionada com a dimensão da organização, mas tendo em conta que, entre os bancos que contribuíram para este estudo, existem alguns de maior dimensão com um número de utilizadores inferior a outros de menor dimensão, este facto não poderá ser usado como justificação para esta divergência quanto ao número de utilizadores. As explicações que puderam ser encontradas durante este estudo relacionam-se, por um lado, com a intenção de alargar a recolha de dados ao maior número de colaboradores possível, garantindo assim uma melhor identificação das fragilidades da instituição (e.g. riscos a que está exposta, eficácia dos controlos implementados), e, por outro, com o desejo/ capacidade da instituição de fazer investimentos menores/ maiores para ampliar o sistema de informação a um número mais elevado de utilizadores – apesar de estes investimentos

não estarem, na maioria dos casos, associados a aspectos tecnológicos, a necessidade de dar formação a um maior número de utilizadores (por vezes, em localizações geográficas distantes) e a indispensabilidade de uma maior alocação de recursos para gerir estruturas de registo e análise mais vastas constituem aspectos susceptíveis de restringir a decisão de expandir a utilização do sistema de informação a um maior número de colaboradores.

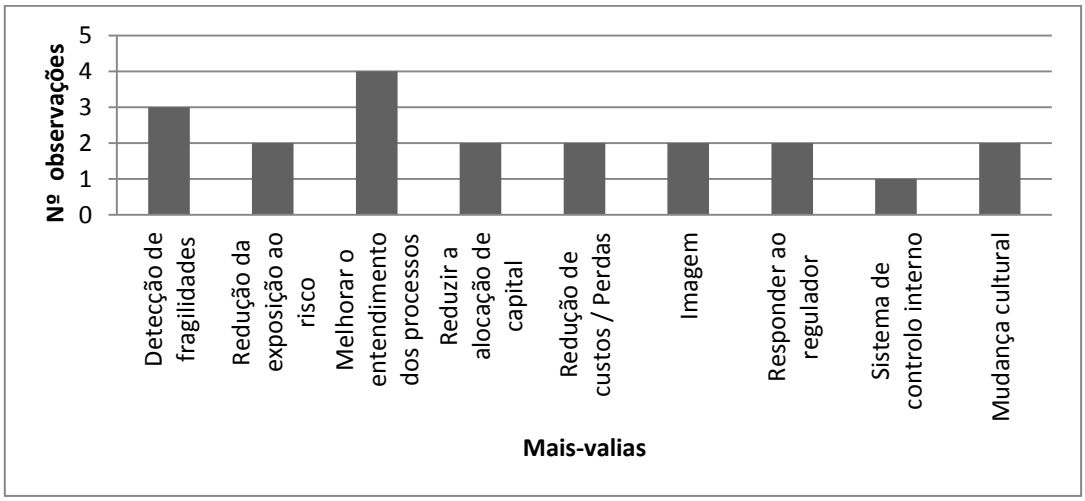
Figura 13 – Utilizadores do sistema de informação de risco operacional na banca



Quando interpelados sobre quais as mais-valias (Figura 14 – Mais-valias da gestão de risco operacional para a banca) que esperavam obter com a gestão de risco operacional e com a implementação de um sistema de informação, os bancos identificaram, como principais, a possibilidade de melhorarem a sua compreensão sobre os seus processos de negócio e a detecção de fragilidades. Estas respostas conduzem à conclusão de que estes bancos estão mais focados na possibilidade de a gestão de risco operacional os ajudar a melhorar a forma como executam as suas actividades do que em responder ao regulador (mais-valia apontada apenas por duas instituições), a razão inicial que os levou a investirem neste risco. Os bancos também reconheceram outras

mais-valias qualitativas, como as questões de imagem, a mudança cultural e o controlo interno – todos estes factores permitem transmitir, interna e externamente, a capacidade da instituição para fazer face a ameaças e oportunidades, bem como para demonstrar a sua concordância com normas e regulamentos na execução das suas actividades. A todos estes pontos de carácter mais qualitativo, juntam-se outras mais-valias de índole mais quantitativa, tais como a redução de custos e perdas e a redução da alocação de capital para risco operacional. Ambos os pontos correspondem a objectivos principais que a gestão de topo quer ver atingidos com o programa de gestão de risco operacional, pois têm impacto directo sobre a rentabilidade e a liquidez da instituição, além de que representam uma justificação objectiva para os investimentos realizados. Tendo sido a necessidade de responder aos requisitos da entidade supervisora a primeira razão para os bancos investirem em programas de gestão de risco operacional, todos os outros pontos identificados pelas diversas instituições demonstram veementemente que também encaram a gestão de risco operacional como uma clara oportunidade de melhoria organizacional que merece investimento, da qual o retorno, ainda que nem sempre se manifeste evidente, é verdadeiramente elevado.

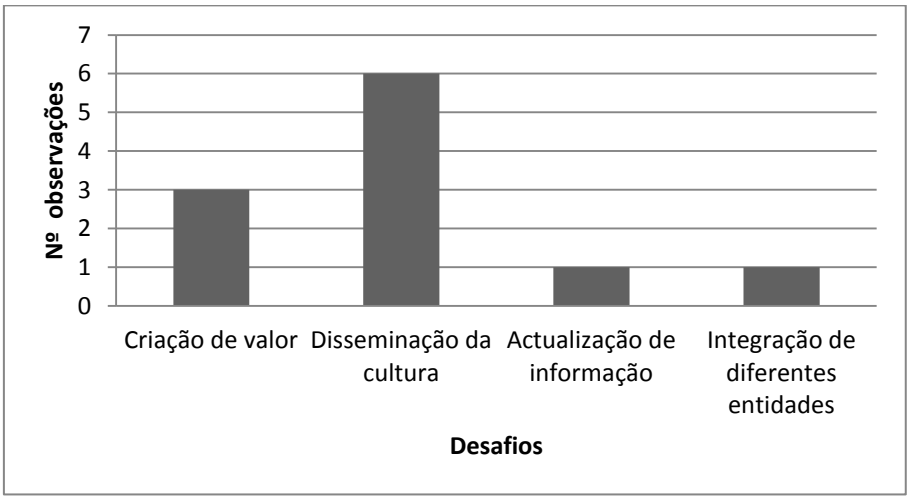
Figura 14 – Mais-valias da gestão de risco operacional para a banca



Foi igualmente pedido aos bancos que identificassem desafios (Figura 15 – Desafios na implementação da gestão de risco operacional na banca) que terão de enfrentar para porem em prática os seus programas de gestão de risco operacional. O repto claramente identificado pela maioria dos bancos equivale à dificuldade em disseminar uma cultura de risco operacional (incluindo mesmo o conceito) por toda a organização, de forma a obter a colaboração de todos os potenciais intervenientes de um programa estruturado – por exemplo, muitas instituições têm grande dificuldade no processo de recolha de dados, porque os intervenientes não entendem nem o seu o objectivo, nem as suas mais-valias, tal como foi apresentado por Haas e Kaiser (2004). Este ponto está intimamente ligado ao número de utilizadores que o sistema tem alocado. Só as instituições que consigam enfrentar o problema cultural é que poderão alargar a utilização do sistema de informação a um maior número de colaboradores e garantir fiabilidade na informação recolhida e nas análises efectuadas. Foram, ainda, identificadas outras contrariedades, a saber: (i) a dificuldade em potenciar a criação de valor através da gestão de risco operacional. Este também constitui um ponto claramente cultural e relacionado com a capacidade do banco para aproveitar toda a informação que é criada por um programa de gestão de risco operacional, a fim de melhorar os seus processos de negócio. Existem dados, como a identificação de riscos ou a eficácia dos controlos, que, se integrados no processo de definição de estratégia ou mesmo nos processos diários, podem garantir uma melhoria da eficácia interna do banco e um melhor relacionamento com clientes e outros intervenientes do mercado. Apesar desta aparente mais-valia, o desafio existe, pois ainda não é clara a forma como esta informação pode ser integrada de modo a trazer um valor real para a instituição – a potencial redução de custos e a menor alocação de capital nos métodos avançados são as mais-valias mais directamente

observáveis. Outro obstáculo reside na (ii) actualização da informação. Este ponto já foi referido no capítulo "Dados Internos" e relaciona-se com aspectos culturais, como o nível de propensão dos colaboradores para registar dados no sistema. Torna-se igualmente crucial desenvolver mecanismos ágeis de integração do sistema de informação de risco operacional com outros sistemas existentes na instituição para a recolha de dados aí registados. A (iii) integração de diferentes entidades em casos de bancos que façam parte de grupos empresariais corresponde a outra das dificuldades apontadas. A capacidade de integrar dados de diversas entidades torna-se complexa, devido a factores tecnológicos (entidades com diferentes sistemas) e à classificação dos eventos e riscos – no caso de não haver uma definição clara das estruturas de registo e das análises para todo o grupo, traduz-se essencial, na fase de integração, efectuar os mapeamentos necessários para que se garanta a integridade e a fiabilidade da base de dados do grupo. Nessa fase de integração, é preciso acautelar também questões de confidencialidade, já que se tratam de eventos recolhidos em diferentes entidades cujo nível de disponibilização tem de ser respeitado.

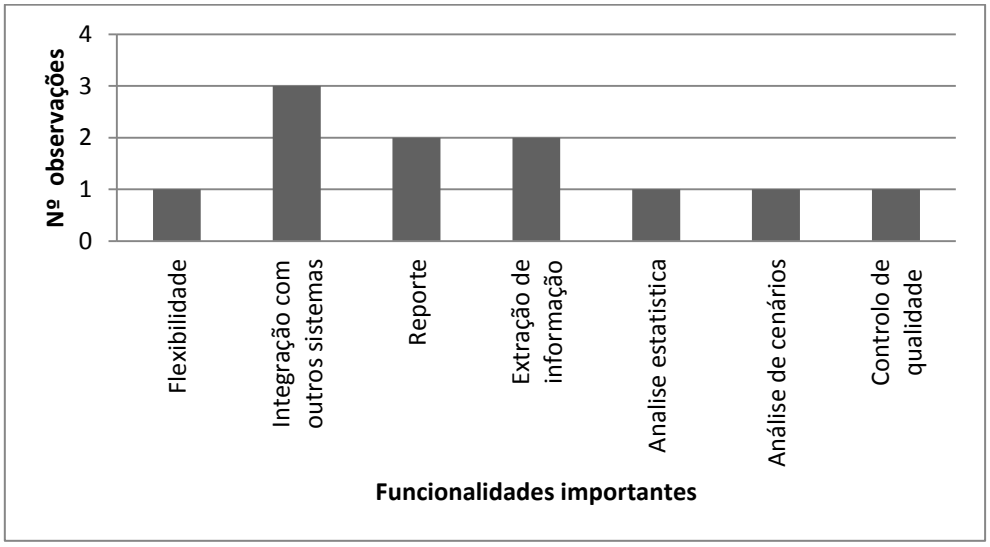
Figura 15 – Desafios na implementação da gestão de risco operacional na banca



Quanto às funcionalidades (Figura 16 – Funcionalidades requeridas pela banca para os seus sistemas de informação para risco operacional) que são consideradas como as mais importantes num sistema de informação para risco operacional, mostram-se muito distintas, consoante os objectivos e a estratégia de cada um dos bancos. Entre as citadas, destaca-se a capacidade de integração com outros sistemas, o que irá, manifestamente, ajudar os bancos a recolher informação que se encontra dispersa pela sua estrutura e a atingir, assim, os objectivos propostos por Mestchian (2003), contribuindo para o desenvolvimento de um base de dados mais robusta que revele o perfil e a exposição ao risco operacional do banco. Esta integração está direccionada para alimentar o sistema de risco operacional com dados armazenados noutros sistemas (e.g. Contabilidade e Help Desk). A integração no sentido oposto, ou seja, ser o sistema de risco operacional a disponibilizar dados a outros sistemas, ainda não foi identificada como uma necessidade – este passo deverá começar a ser implementado, quando os bancos definirem uma metodologia para a integração de dados de risco operacional no seu processo de negócio. Existe também um conjunto de funcionalidades identificadas, mais relacionadas com a facilidade e flexibilidade na utilização dos sistemas, bem como com o acesso à informação que estes podem facultar (e.g. Reporte) – sem dúvida que estas se encontram directamente ligadas ao desafio cultural que foi identificado pelos bancos, enquanto o seu maior obstáculo, e à sua tentativa de alargar e tornar mais acessíveis os conceitos e as metodologias do risco operacional ao maior número de colaboradores possíveis. Este ponto vai exercer impacto directo sobre a capacidade da instituição para captar eventos e indicadores de risco. Para os bancos que ponderam começar a desenvolver análises e métodos mais avançados, as funcionalidades estatísticas e de cenários apresentadas por Gibson (1997) revestem-se de elevada importância. É relevante destacar que três dos bancos consultados declararam não sentir a necessidade

de ter mais funcionalidades do que aquelas que os seus actuais sistemas disponibilizam – ou seja, recolha de eventos, questionários de auto-avaliação e indicadores de risco –, o que poderá indiciar que, nestes casos, o sistema de risco operacional possui como único objectivo a recolha de dados (poderão existir outras áreas que utilizem estes dados para as suas actividades).

Figura 16 – Funcionalidades requeridas pela banca para os seus sistemas de informação para risco operacional



Como nota final, sobressai a existência, na totalidade dos bancos, de sistemas para a gestão de risco operacional, todos eles com capacidades que permitem uma potencial aprovação por parte do supervisor. No entanto, o supervisor poderá identificar pontos, como o nível de segregação de funções, passíveis de influenciar o processo de aprovação. Afigurou-se, também, evidente que, para a maioria dos inquiridos, a gestão de risco operacional não é algo que, apesar de assumido pelos níveis mais elevados das instituições, se encontre já com um processo perfeitamente definido e cujos objectivos a longo prazo estejam claramente estabelecidos. Nesse sentido, as áreas responsáveis pelo

risco operacional vêem nos sistemas de informação um factor susceptível de as ajudar a alavancar um trabalho de base, já em curso, mas sobre o qual ainda podem ser desenvolvidos processos que levem o risco operacional a ser considerado, de forma mais evidente e directa, como um factor crítico de sucesso para as instituições.

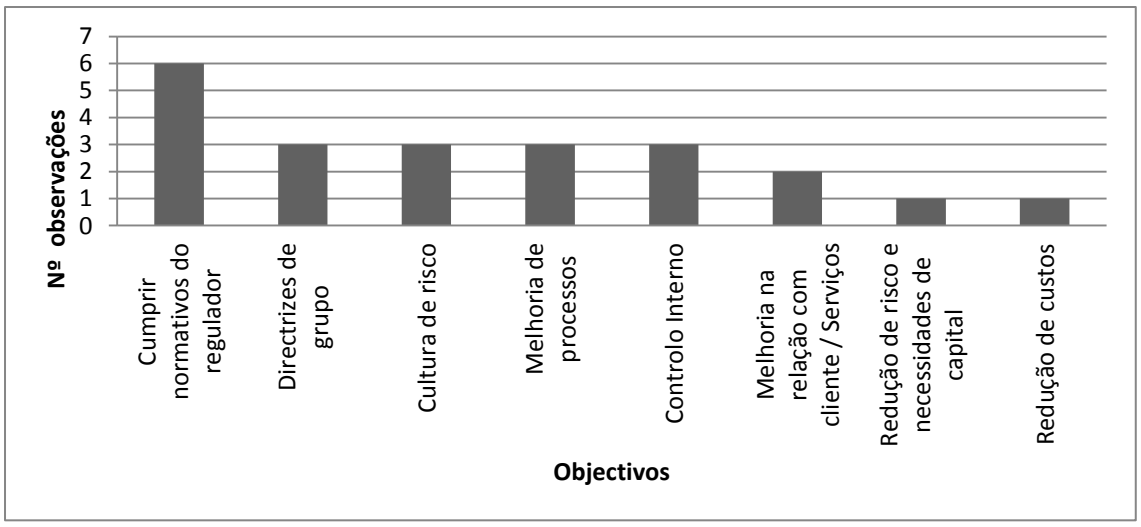
5.2.2 – Instituições Seguradoras

Para as instituições seguradoras, ainda não se verifica um evento compulsivo que as impulsione, desde já, a implementar programas de risco operacional – o Acordo Solvência II ainda não se encontra em vigor. No entanto, todas as seguradoras que contribuíram para este estudo já se afirmam conscientes da necessidade de incluir o risco operacional nos seus planos estratégicos e investimentos. As respostas obtidas revelaram existir uma disparidade entre um grupo de instituições já em estágio avançado de processo de implementação e outro que começa dar os primeiros passos nas suas abordagens.

Em relação à questão sobre quais os objectivos da gestão de risco operacional (Figura 17 – Objectivos da gestão de risco operacional nas seguradoras) para as instituições seguradoras, os resultados obtidos assemelham-se bastante aos da banca. Cumprir com os requisitos do regulador, mesmo que estes não se encontrem definitivamente estabelecidos, perfaz algo claramente identificado por todas as seguradoras como um dos objectivos principais para avançarem para um sistemático processo de gestão de risco operacional e para a implementação de um sistema de informação. Na sua quase totalidade, as seguradoras inquiridas pertencem a grupos económicos nos quais também estão presentes bancos, ou a grupos internacionais cujas implementações lhes fornecem linhas orientadoras para os seus desenvolvimentos. Esta

foi também a razão que levou algumas seguradoras a indicar o ponto "responder a directrizes de grupo" como um dos seus objectivos – relacionado com os requisitos dos supervisores das empresas mãe. Os outros objectivos identificados apresentam uma perspectiva essencialmente qualitativa, como o desenvolvimento da cultura de risco dentro da instituição – área igualmente revista essencial na banca –, o melhoramento dos seus processos e o fomento do controlo interno, assegurando, assim, credibilidade perante as empresas de *rating*, o supervisor e o mercado em geral (Helbok & Wagner 2006). Por fim, foram ainda reconhecidos objectivos de eficácia operacional, como a melhoria na relação com os clientes e nos serviços prestados, a redução da exposição aos riscos, das necessidades de capital e de custos. Estes dois últimos pontos são objectivos gerais de um programa de gestão de risco operacional.

Figura 17 – Objectivos da gestão de risco operacional nas seguradoras



No tocante às abordagens actuais e futuras que as seguradoras estão e pensam seguir, existe uma grande consistência entre todas as instituições consultadas. Relativamente à abordagem actual, as seguradoras encontram-se a seguir o definido

pelo Instituto de Seguros de Portugal (ISP), a sua entidade supervisora, que, através da norma 14/2005-R, estabeleceu os requisitos actuais em relação à gestão de risco operacional (as respostas "não definido" por parte de certas instituições devem-se ao facto de estas não verem esta norma como algo específico para risco operacional). Em relação ao futuro, existe uma clara indefinição quanto à abordagem a seguir. A causa fundamental é o Acordo Solvência II ainda não ter sido dado como concluído, o que deixa as seguradoras com um elevado grau de incerteza perante o que virão a ser os requisitos finais do Acordo e os reais benefícios de cada uma das abordagens disponíveis. Como é esperado que o Solvência II apresente no caso do risco operacional directrizes muito semelhantes ao Basileia II, as seguradoras estão a estruturar-se para responder a requisitos idênticos aos que foram definidos pelo supervisor para a banca. Nesse sentido, existe uma das seguradoras que já equaciona os métodos avançados como abordagem futura, com o objectivo de atingir níveis de capital mais reduzidos para alocar a risco operacional.

No que concerne à forma como as seguradoras se estão a organizar para responder à gestão de risco operacional, a opção de a colocar dentro da Direcção de Risco (quatro instituições) é, neste momento, a que prevalece perante outras, tais como remetê-la para a direcção de Controlo Interno (uma instituição) ou para órgãos conjuntos (duas instituições). A razão que pôde ser apurada durante este estudo baseia-se no facto de ser na Direcção de Risco que se irá centrar a problemática do Acordo Solvência II.

Tal como na banca, a estratégia seguida pelas seguradoras para a recolha de informação no seu processo de gestão de risco operacional é descentralizada, em muito justificada pelos factores expostos por de Fontnouvelle (2006) e Allen e Bali (2004). Apesar de ser um processo mais recente do que na banca, os programas de risco operacional parecem ter sido mais facilmente integrados nas seguradoras, o que veio

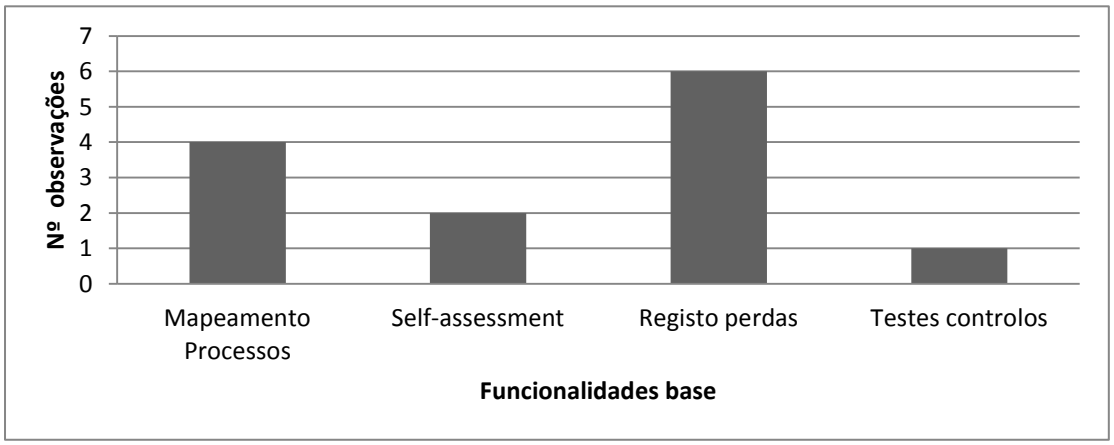
facilitar um processo de recolha de informação mais descentralizado – é preciso, no entanto, referir que, na maioria dos casos, o próprio nível de dispersão da estrutura da seguradoras traduz-se significativamente inferior ao da banca, o que também serviu como facilitador para o desenvolvimento de estratégias mais descentralizadas (menor número de localizações geográficas e utilizadores).

Quanto à existência de um sistema de informação para suporte à gestão de risco operacional, existe já uma preponderância entre as seguradoras que já o possuem relativamente às que não o têm – ao contrário do que sucede na banca, ainda existem duas seguradoras sem um sistema de informação que suporte o seu processo de gestão de risco operacional (podem existir, porém, repositórios de dados de eventos de risco operacional dispersos pela organização). O facto de já se verificarem instituições com sistemas de informação pode ser explicado através das directrizes apontadas pelos documentos relacionados com o Acordo Solvência II (KPMG 2002), que realçam o imperativo de fazer investimentos nessa área. O grau de sofisticação destas implementações relaciona-se, directamente, com três factores: a dimensão da seguradora, a existência de directrizes de grupo, ou a visão dos órgãos de gestão para a sua necessidade. As seguradoras mais avançadas na implementação dos seus sistemas de informação para risco operacional reviram nestes um meio para melhorarem a sua imagem, tanto no mercado, quanto perante as empresas de *rating*, ou para respeitar critérios de controlo de qualidade. O passo seguinte será a utilização de toda a informação disponível com vista a incorporarem-na nos seus processos de negócio, ao mesmo tempo que garantem, atempadamente, a sua resposta aos requisitos impostos pelo supervisor, ao abrigo do Solvência II.

Nas funcionalidades (Figura 18 – Funcionalidades base dos sistemas de informação para risco operacional nas seguradoras) mais requeridas pelas seguradoras nos seus

sistemas de informação para gestão de risco operacional, o registo de perdas ganha uma clara preponderância, pois as seguradoras vêem-na como o ponto de partida para começarem a construir a sua base de dados de risco operacional (Mestchian 2003), o que as irá apoiar no seu processo de identificação dos riscos, níveis de frequência e de severidade. O mapeamento de processos é uma funcionalidade que quatro seguradoras reconhecem fundamental para as ajudar a incrementar o seu conhecimento da instituição e a garantir o alinhamento de diferentes direcções (e.g. Auditoria Interna, Organização) sob o mesmo conjunto de informação, assegurando, assim, economias de escala na implementação de sistemas que suportem estas áreas, bem como transparência e integridade no reporte que é produzido. Associadas a estas estão outras duas funcionalidades identificadas por algumas seguradoras: *self-assessment* (duas instituições) e testes aos controlos (uma instituição), que também constituem fontes de identificação de riscos e fragilidades, as quais garantem um conhecimento mais pleno da instituição e a colaboração entre diversas direcções.

Figura 18 – Funcionalidades base dos sistemas de informação para risco operacional nas seguradoras

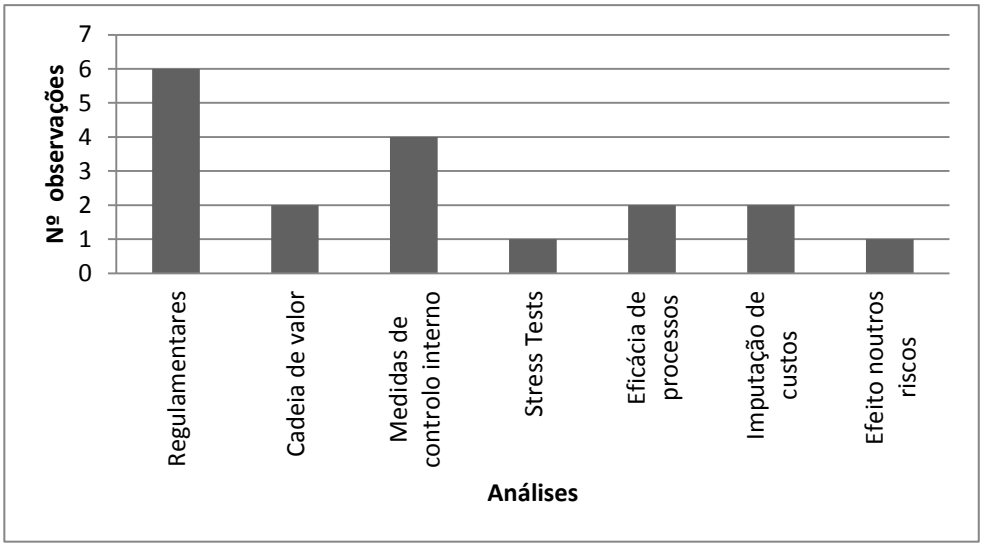


Quanto às fontes de dados utilizadas para alimentar os sistemas de informação, constata-se uma clara tendência para o carregamento manual de dados (cinco instituições), existindo já duas seguradoras que também recorrem aos dados dos seus sistemas operacionais para alimentar a base de dados de risco operacional. Tal como na banca, o carregamento manual tem sido o método privilegiado pelas instituições seguradoras para começarem a recolher informação rumo à construção da sua base de dados, recorrendo a conhecimento que se encontra disperso na organização e que, pela primeira vez, começa a ser estruturado. No que respeita à possibilidade de integração com outros sistemas, duas seguradoras já o efectuam, tendo mesmo desenvolvido mecanismos que, quase em tempo real, permitem a troca de informação entre diferentes sistemas (e.g. sistema de risco operacional e sistema de reclamações). Seguradoras que venham a ter uma cultura de risco mais abrangente e programas de risco operacional mais ambiciosos poderão vir a implementar, no seu sistema de informação, mecanismos automáticos de recolha de informação de outros sistemas operacionais, procurando, desta forma, colmatar alguns dos desafios na construção da sua base de dados, como os apresentados por Marshall (2001).

De entre as análises que as instituições de seguros identificaram como as mais importantes (Figura 19 – Análises de risco operacional nas seguradoras) para a sua gestão de risco operacional, destacam-se as requeridas pela entidade supervisora. Este tem sido, numa primeira fase, o principal objectivo das seguradoras para as análises do seu sistema de informação. Embora o Acordo de Solvência II ainda não se encontre finalizado, pretendem assegurar, desde já, a capacidade do seu sistema para responder aos requisitos que se esperam que sejam incluídos no Acordo. No entanto, e como também se pôde observar a partir da análise aos objectivos das seguradoras para os seus programas de risco operacional, estas identificam um conjunto de análises para as

ajudar a gerir melhor o seu negócio. Neste caso, sobressaem as medidas para a análise da eficácia do controlo interno, a eficiência de processos e a imputação de custos. Estas três análises permitem à instituição avaliar a sua capacidade de controlar e mitigar a sua exposição a risco operacional, através dos seus mecanismos internos, e utilizar os resultados destas análises para avaliar a performance de produtos ou linhas de negócio por meio da imputação de custos a estas dimensões, de acordo com os níveis de risco a que se expõem e com a sua capacidade de controlar e mitigar risco. Com base na experiência que as instituições seguradoras possuem na gestão de risco, é expectável que, no futuro, venham a desenvolver novas metodologias de análise que lhes permitam incorporar os seus indicadores de risco operacional directamente no seu negócio (e.g. cálculo de prémios ou comissões de mediadores).

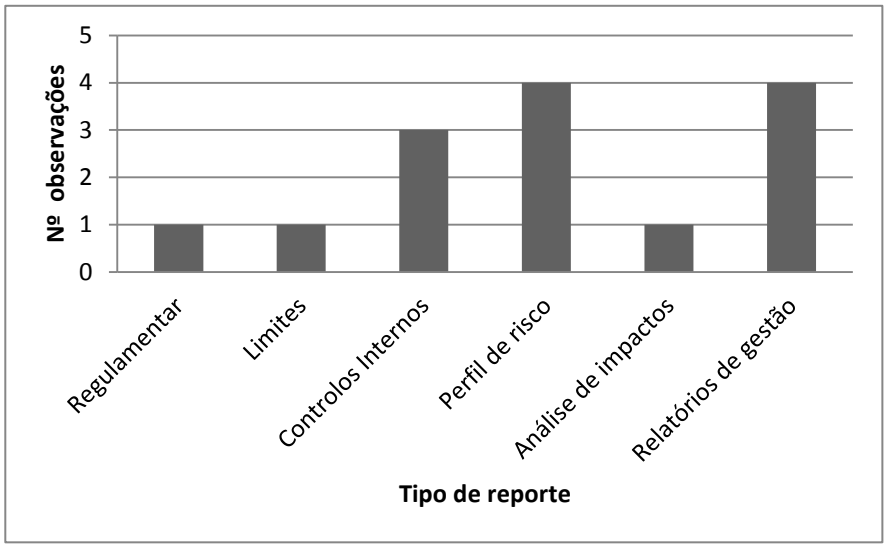
Figura 19 – Análises de risco operacional nas seguradoras



Quando se analisa o reporte (Figura 20 – Reporte requerido para risco operacional por parte das seguradoras) identificado pelas seguradoras como o mais importante a retirar dos seus sistemas de informação para risco operacional, percebe-se claramente

uma maior preocupação com a gestão da instituição do que com os requisitos regulamentares – algo que parece ir em sentido contrário ao que fora identificado na abordagem à questão das análises. No entanto, este ponto pode encontrar a sua explicação no facto de ainda não existirem as especificações finais para o reporte que será exigido pelo supervisor, o que faz com que as seguradoras estejam mais preocupadas em retirar informação de gestão sobre os seus controlos internos, ou sobre o perfil de risco da sua actividade – indicadores que lhes irão permitir desenvolver uma cultura interna de risco operacional, melhorar a sua actividade, reduzir custos e garantir um melhor serviço e imagem perante o mercado. Todos estes pontos foram identificados como objectivos para os programas de risco operacional da maioria das seguradoras inquiridas; estão, além disso, em linha com os resultados apresentados pelo estudo da Risk Magazine (2003), que aponta a melhoria na eficiência e resultados como um dos principais objectivos das instituições para os seus programas de risco operacional. Esta análise pode traduzir-se num indicador importante para nos ajudar a entender a metodologia das seguradoras perante o risco operacional, mostrando que, mesmo considerando a necessidade de responder aos requisitos do regulador, as seguradoras entendem fundamental utilizar toda a informação que irão recolher para as auxiliar a melhorar as suas actividades.

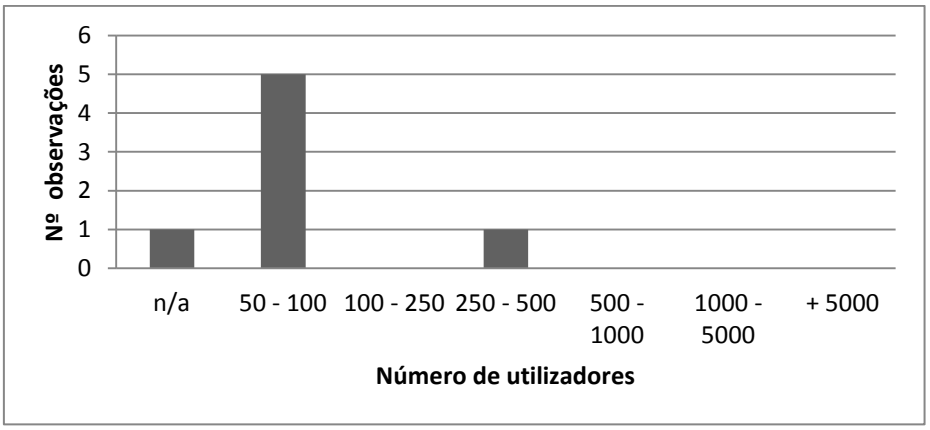
Figura 20 – Reporte requerido para risco operacional por parte das seguradoras



Quanto ao número de utilizadores credenciados para usar o sistema de informação de risco operacional nas seguradoras (Figura 21 – Número de utilizadores dos sistemas de informação de risco operacional nas seguradoras), a maioria (cinco instituições) tem entre 50 e 100 dos seus colaboradores a interagir com o sistema de informação. Este número parece associar-se à dimensão da própria instituição. No futuro, esta questão poderá, porém, apresentar resultados diferentes, após a entrada em vigor do Acordo Solvência II e o desenvolvimento da cultura de risco operacional nas instituições. Foi possível observar neste estudo que, na sua grande maioria, as instituições seguradoras estão a abordar o tema do risco operacional com alguma prudência e, no que toca à difusão do sistema de informação aos seus colaboradores, preferem concentrar-se em estratégias mais circunscritas, com direcções específicas e elementos-chave a contribuir para este sistema de informação. Os desenvolvimentos que estão presentemente a ser realizados não só garantem um conjunto inicial de informação sobre o estado da instituição relativo ao seu processo de gestão de risco operacional (indicativo do que poderá vir a ser uma implementação mais alargada), como lhes permitem responder aos

requisitos actuais do supervisor (norma 14/2005 – R). A seguradora que já dispõe de um número de utilizadores entre os 250 e os 500 encontra-se numa fase mais avançada do desenvolvimento do seu programa de risco operacional e do seu sistema de informação, além de estar integrada num grupo económico que definiu este programa como um ponto fulcral da sua estratégia.

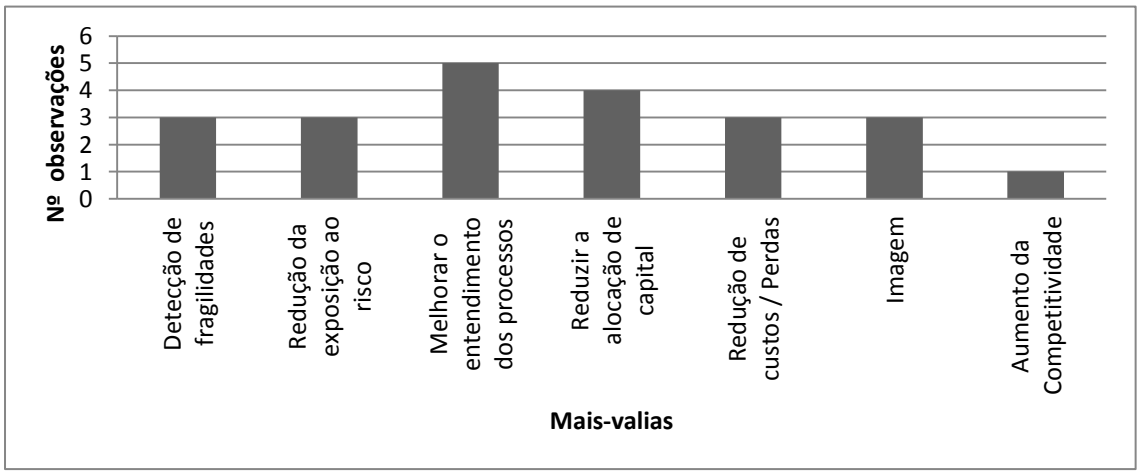
Figura 21 – Número de utilizadores dos sistemas de informação de risco operacional nas seguradoras



A partir da análise às mais-valias da gestão de risco operacional (Figura 22 – Mais-valias da gestão de risco operacional para as seguradoras) identificadas pelas seguradoras, pôde confirmar-se a tendência de que estas instituições vêem a gestão de risco operacional enquanto forte competência para as ajudar a aperfeiçoar a sua actividade, reduzir os efeitos financeiros do risco operacional e melhorar a sua imagem no mercado. As seguradoras mostram-se essencialmente preocupadas em aumentar o conhecimento que têm sobre si próprias, através do cultivo de uma noção mais profunda quer dos seus processos de negócio (identificação de riscos por processo e dos controlos implementados para os mitigar), quer das suas fragilidades (níveis de exposição a riscos e falta de efectividade dos controlos). Outro conjunto de mais-valias inclui elementos

mais quantitativos, como a redução da exposição ao risco e, associado a este, a redução das perdas e da severidade destas. Como resultado final do processo de gestão de risco, as seguradoras esperam também conseguir uma redução no capital a alocar para risco operacional, ao abrigo do Acordo Solvência II. A gestão de risco operacional é vista, outrossim, por algumas seguradoras (três instituições) como um método eficiente para apoiá-las a melhorar a sua imagem – algo que é sustentado pelos documentos, tanto das entidades supervisoras (norma 14/2005 – R), quanto das empresas de *rating* (Moody's Analytical Framework for Operational Risk Management of Banks, 2003; Operational Risk Management & Basel II implementation: Survey Results, 2004).

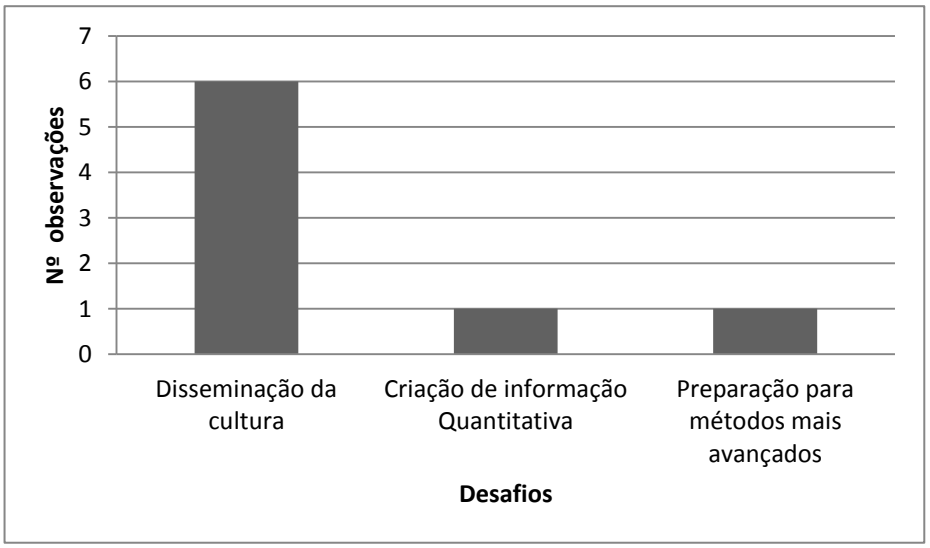
Figura 22 – Mais-valias da gestão de risco operacional para as seguradoras



Tal como nos bancos, também nas seguradoras o grande desafio (Figura 23 – Desafios para a gestão de risco operacional nas seguradoras) identificado pela maioria (seis instituições) corresponde à sua capacidade para disseminar uma cultura de risco operacional (um dos principais problemas, apresentados por Haas e Kaiser (2004), que emerge da recolha de dados). Criar, nos intervenientes deste processo, a consciência da

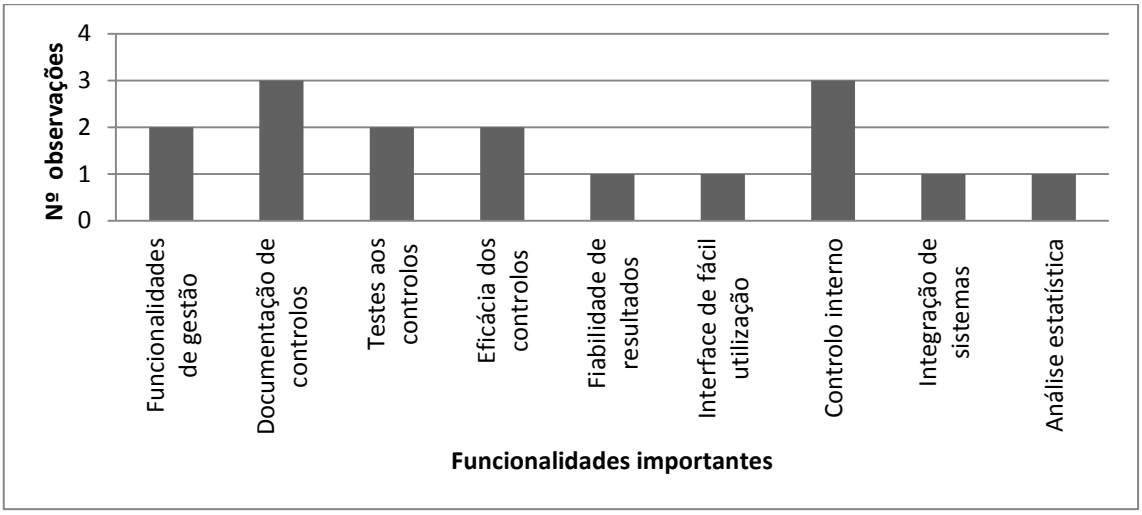
importância e das razões pelas quais se deve gerir risco operacional continua, e possivelmente continuará, a ser o grande repto para estas instituições – processos de formação e de disseminação dos resultados obtidos com o programa de gestão de risco operacional podem ajudar a mitigar este problema. Foi também identificado um desafio na área da transformação de informação qualitativa em quantitativa – circunstância muitas vezes ligada à dificuldade em entender os conceitos e os impactos do risco operacional para conseguir abordar questões qualitativas, ou à coerência e exactidão dos resultados obtidos pelos métodos qualitativos, tal como foi apresentado por Hubbard (2009). O desafio da preparação para métodos avançados é, na prática, uma consequência da necessidade de disseminar a cultura – uma seguradora só poderá estar preparada para responder a abordagens mais avançadas quando toda a organização reconhecer o risco operacional como uma das suas áreas vitais e, deste modo, conseguir estar estruturada para recolher, analisar e gerir a informação que os métodos avançados exigem. Também deverão ser esperados, nos métodos avançados do Solvência II, os mesmos reptos já identificados para os (AMA) de Basileia II, previamente apresentados neste trabalho, no capítulo "Modelação e quantificação de Risco Operacional".

Figura 23 – Desafios para a gestão de risco operacional nas seguradoras



Nas funcionalidades mais importantes requeridas pelas seguradoras para os seus sistemas de gestão de risco operacional (Figura 24 – Funcionalidades mais importantes nos sistemas de risco operacional para as seguradoras), o controlo interno toma clara relevância. Foram identificados não só o tópico do controlo interno, como todo um conjunto de funcionalidades a ele associadas, tais como a documentação de controlos, os testes aos controlos e a análise à sua eficácia. Parece evidente que as instituições seguradoras desejam aproveitar os seus sistemas de informação para risco operacional e a informação por eles fornecida para melhorar todos os aspectos referentes ao seu controlo interno, de forma a reduzir custos e perdas e garantir processos, produtos e serviços de melhor qualidade. Aqui desempenha um papel fundamental o ponto, já apresentado, referente ao alargamento da utilização destes sistemas às direcções de Auditoria Interna e de *Compliance*, uma vez que estas duas direcções são em muito responsáveis pela garantia do correcto funcionamento dos mecanismos de controlo interno e pelo reportar ao supervisor e ao mercado dos níveis de implementação e eficácia destes mecanismos. As outras funcionalidades identificadas podem ser agrupadas em dois grupos principais: (i) as que se referem à melhoria no processo de recolha de dados, através quer de interfaces de fácil utilização (para diminuir a resistência já identificada no processo de reportar eventos), quer da integração com outros sistemas operacionais (e.g. reclamações), e (ii) as associadas à capacidade de produzir informação de gestão à altura de apresentar resultados fiáveis e análises estatísticas passíveis de trazer valor para o processo de gestão de risco operacional da instituição.

Figura 24 – Funcionalidades mais importantes nos sistemas de risco operacional para as seguradoras



Revelou-se notório neste estudo que, à excepção de uma das seguradoras que participaram, todas as outras se encontram nos estágios iniciais de evolução dos seus programas de risco operacional e dos sistemas de informação que os irão suportar. Este facto, aparentemente relacionado com o atraso na apresentação do documento final do Acordo Solvência II, tem vindo a inspirar alguma prudência por parte das diferentes instituições no desenvolvimento dos seus programas. No entanto, todas as seguradoras parecem ter bem identificada a necessidade de implementarem programas de gestão de risco operacional que lhes permitam, mais do que responder ao supervisor, melhorar a sua actividade e os seus resultados, essencialmente através da redução de perdas por risco operacional e da racionalização dos custos com o controlo interno. Outro ponto que se destacou desde as etapas iniciais do processo de implementação do sistema de informação foi a existência de uma colaboração estruturada e de uma integração de dados entre a direcção de risco e outras direcções (e.g. Auditoria Interna, Organização), de forma a potenciar a utilização de funcionalidades e dados comuns.

5.2.3 – Entidades Reguladoras

Este capítulo destina-se a avaliar a visão que ambas as entidades reguladoras (BdP e ISP) têm no que respeita a gestão de risco operacional e os sistemas de informação passíveis de a suportar. A interpretação é feita de forma agregada, com o objectivo de não expor directamente a posição de cada uma das entidades.

De seguida, são analisadas cada uma das questões colocadas aos reguladores portugueses.

1. Como vê a entidade reguladora a gestão do risco operacional nas diferentes instituições? Os dois reguladores, mesmo antes da promulgação da actual legislação, consideravam o risco operacional como uma área que devia ser analisada dentro das instituições que supervisionam. Reconhecem, no entanto, que quer o Acordo Basileia II para a banca, quer o Solvência II para os seguros vieram trazer um novo dinamismo e uma sistematização importante para a gestão de risco operacional. Este facto é conseguido não apenas pelos novos requisitos de alocação de capital para risco operacional, mas essencialmente pelos requisitos qualitativos e de gestão que são exigidos aos bancos e às seguradoras para poderem prosseguir para abordagens mais avançadas. As diferentes instituições deverão ter a capacidade de identificar, avaliar e controlar o seu risco operacional, de modo a obter uma compreensão bastante fiel do seu perfil de risco. A gestão de risco operacional deverá ter uma natureza preventiva, de forma a prevenir perdas e custos de origem operacional, bem como garantir ganhos de eficiência operativa.

2. Qual a abordagem regulamentar que prevê que as instituições irão seguir? Neste momento, os reguladores esperam que, na sua maioria, as entidades que supervisionam se candidatem aos métodos standard, em que terão de desenvolver políticas e procedimentos internos para a gestão do risco operacional, mas onde as exigências para o cálculo de requisitos de capital não são tão elevadas como nos métodos avançados. Existe ainda uma grande dúvida sobre o número de entidades que, no futuro, irão apresentar a sua candidatura aos métodos avançados. Só com o decorrer do tempo, e com as diferentes implementações, se poderá verificar a capacidade e as vantagens que as instituições poderão vir a ter se avançarem para abordagens mais sofisticadas – nem sempre as vantagens teóricas se reflectem na prática.
3. Qual a importância que a entidade reguladora irá dar à existência de um sistema de informação para a gestão de risco operacional? Tanto o BdP como o ISP reconhecem a relevância de sistemas de informação que assegurem níveis elevados de capacidade, performance e segurança, assim como a fiabilidade e consistência da informação recolhida. A eficácia destes sistemas de informação deverá ser adequada à dimensão, à complexidade das actividades e aos riscos de cada uma das instituições. Um sistema de informação para risco operacional é reconhecido como vital para as instituições que se candidatem às abordagens avançadas.
4. Quais as funcionalidades base que vê com maior importância neste tipo de sistemas? As diferentes instituições deverão ser capazes de identificar, avaliar, controlar e monitorizar a exposição ao risco operacional. Assim, espera-se que o sistema de informação apoie a recolha de eventos de perda e recuperação, no desenvolvimento de exercícios de auto-avaliação de riscos e controlos, assim

como possua funcionalidades para compilar factores relativos ao contexto económico e ao sistema de controlo interno. Deverá também permitir que sejam desenvolvidos cenários que reflictam a exposição a riscos de elevada severidade, ainda que apresentem uma reduzida probabilidade de ocorrência. Os sistemas de informação deverão, inclusive, representar um papel fundamental no processo de determinação do nível de capital mais adequado para fazer face à potencial ocorrência de risco operacional.

5. Quais os grandes desafios da gestão de risco operacional? Também para os reguladores, a criação de uma cultura de risco operacional apresenta-se como um dos maiores desafios colocados à gestão do risco operacional, na medida em que, se não for devidamente interiorizada pelos diferentes colaboradores das instituições, todo o processo, desde a recolha de informação, até ao nível de identificação de medidas de mitigação, pode ser claramente posto em causa. As dificuldades inerentes à modelação do risco operacional estão associadas a razões como a falta de informação recolhida sobre risco operacional, os desafios colocados pela necessidade de integração de dados internos, externos e cenários, bem como a análise de efeitos de correlação e diversificação – todos estes factores serão uma forte condicionante nos resultados da gestão de risco operacional, que tem de ser correctamente endereçada pelas instituições e pelos seus sistemas de informação. Torna-se igualmente indispensável alertar para a importância de os níveis de gestão de topo se envolverem activamente na gestão do risco operacional, desde a definição da estratégia global da instituição à aplicação de planos de acção. Outro desafio que pode ser significativo traduz-se na escassez de recursos para trabalhar este "novo" risco.

6. Quais as mais-valias de uma gestão do risco operacional para a entidade reguladora? É objectivo das entidades reguladoras defender a estabilidade e a integridade do sistema onde actuam, assegurando ao mercado que as instituições que supervisionam têm níveis mínimos de solvabilidade compatíveis com o risco que integram. No caso do risco operacional, espera-se que as instituições possam evitar, através da gestão eficiente deste risco, perdas inesperadas e melhorar a eficiência operacional, promover a utilização produtiva do capital e assegurar a vantagem competitiva face à concorrência, proporcionando, em simultâneo, um maior retorno aos accionistas e o reconhecimento do mercado. A gestão do risco operacional deve ser encarada pelas instituições bancárias e seguradoras como uma ferramenta de gestão indispensável no seu dia-a-dia.

5.2.4 – Considerações finais sobre os resultados obtidos

Os resultados obtidos das entrevistas a estas instituições revelaram que a gestão de risco operacional é já considerada vital no desenrolar das actividades usuais de bancos e seguradoras. Apesar do que Buchelt e Unteregger (2004) argumentam, e com base no que foram as respostas sobre objectivos e funcionalidades dos sistemas de informação, pode-se concluir que foram as pressões regulamentares as primeiras a compelirem estas instituições para começar a gerir o seu risco operacional. Mas os bancos e as seguradoras estão a aproveitar os investimentos que tiveram que realizar em recursos e sistemas de informação para tentarem obter informação que lhes permita melhorar o seu conhecimento sobre processos internos e sobre a exposição a riscos internos e externos, tornando, assim, exequível implementar medidas que potenciem melhorias nas suas actividades.

Na sua maioria, os bancos encontram-se mais avançados nesta área, essencialmente devido ao facto de o Acordo Basileia II já se encontrar em vigor. No entanto, também as seguradoras, em antecipação ao Acordo Solvência II, começam a pôr em prática programas de gestão de risco operacional. Afigurou-se interessante analisar que, enquanto na maioria dos bancos o risco operacional foi claramente deixado para segundo plano, ultrapassado pelo risco de crédito e de liquidez, nas seguradoras o risco operacional está a ser dos primeiros a ser considerado na resposta aos requisitos regulamentares.

O facto de os bancos se apresentarem mais avançados reflecte-se na existência de sistemas de informação para risco operacional – a totalidade dos bancos questionados já conserva um sistema de informação para a gestão do seu risco operacional – e no número de colaboradores a interagirem com esse sistema de informação. Os bancos parecem, contudo, numa primeira fase, mais preocupados em garantir a resposta aos requisitos da entidade reguladora; esta intenção repercute-se nas funcionalidades e análises existentes e pretendidas nos seus sistemas. As seguradoras, ainda sem semelhantes pressões regulamentares, parecem igualmente importadas em garantir, desde já, um sistema que lhes assegure ir ao encontro dos requisitos do supervisor, embora concentrem também os seus esforços para acautelar que os seus sistemas de informação lhes fornecem dados que lhes permitam gerir de melhor forma o seu negócio. Apesar do facto já mencionado de as seguradoras estarem a restringir mais o acesso ao sistema de informação do que os bancos, assiste-se nestas a uma maior tendência para começar a agregar no sistema as necessidades de outras direcções, como é o caso da auditoria interna ou a área de *Compliance*.

O principal desafio identificado pelas instituições de ambos os sectores foi a necessidade de difundir uma cultura de risco operacional dentro da organização, que

parece exercer um impacto significativo na capacidade das instituições para o seu processo de recolha de dados e na capacidade de integrar os resultados do seu programa de risco operacional nos seus processos de negócio. Talvez por essa razão o autor pôde observar que nas inúmeras implementações já em curso tem havido um enorme foco nas especificações relativas às funcionalidades aplicacionais do interface e na facilidade da sua utilização, em detrimento de funcionalidades para análise à informação recolhida.

Quanto às entidades reguladoras, é unânime a opinião de que o risco operacional se tornará num alvo preferencial da sua actividade de supervisão e de que a existência de sistemas de informação se revela vital na arquitectura que as instituições financeiras vão ter de implementar a fim de suportar a sua actividade de gestão de risco operacional. Também os supervisores identificam o desenvolvimento de uma cultura de risco operacional como o principal desafio que as instituições terão de enfrentar, mas concluem que todos os desafios devem ser ultrapassados, pois as mais-valias de um programa de gestão de risco operacional são primordiais não só para a sobrevivência de cada instituição, como para o reconhecimento da qualidade da sua gestão pelo supervisor e pelo mercado em geral.

No estudo apresentado há limitações que é necessário considerar para efeitos de conclusões e investigação futura:

1. A amostra reflecte as opiniões e a visão das pessoas que estão directamente ligadas ao risco operacional ou à implementação de sistemas de informação para a sua gestão. No futuro, será necessário considerar outras áreas indirectamente ligadas, através do impacto que a gestão de risco operacional tem na sua actividade (e.g. linhas de negócio);
2. As instituições financeiras mostram-se ainda muito influenciadas por aquelas que são as directrizes dos Acordos de Basileia II e Solvência II.

Assim, as suas metodologias de gestão de risco operacional, bem como a utilização de sistemas de informação estão em muito condicionadas por este facto;

3. A utilização de sistemas de informação para a gestão de risco operacional ainda é recente em Portugal. Desta forma, ainda não existe maturidade suficiente para se poderem alcançar conclusões que sejam fortes indicadores de práticas ou metodologias;
4. Apesar de a amostra utilizada pretender ser representativa dos sectores bancário e segurador em Portugal, não inclui a totalidade das instituições financeiras portuguesas, podendo estar, de alguma forma, enviesada relativamente a instituições menos evoluídas na sua gestão de risco operacional, ou a instituições cuja casa mãe é uma empresa internacional, na qual a gestão de risco operacional é centralizada. No caso das seguradoras, como já mencionado, a futura investigação deverá recolher dados de um maior número de instituições para que se possam obter resultados mais robustos.

V PARTE – DESENHO FUNCIONAL DE UM SISTEMA DE INFORMAÇÃO PARA RISCO OPERACIONAL

6 – DESENHO FUNCIONAL

Ainda não existe um trabalho sistemático que permita apresentar um desenho do que deverá ser um sistema de informação para gestão de risco operacional; há apenas a identificação de um conjunto de funcionalidades, como as que foram descritas ao longo deste trabalho, que têm servido de base para as empresas fornecedoras de software desenvolverem as suas soluções. De igual forma, ainda não existe investigação estruturada que permita desenvolver um conjunto de conhecimento para que se possa apresentar um desenho funcional formal de um sistema de informação para gestão de risco operacional. Este trabalho pretende colaborar para essa investigação, apresentando um desenho funcional para um sistema de informação para gestão de risco operacional em instituições financeiras baseado em duas grandes perspectivas: as linhas identificadas pela investigação académica já realizada e os requisitos apurados através do grupo de entrevistas realizadas às instituições e às entidades reguladoras. Como base metodológica, será utilizada a *Soft System Methodology,* que se apresenta como a mais adequada para responder ao modelo conceptual que integra o objectivo do estudo. Partindo das duas perspectivas apresentadas, serão fornecidas respostas às questões colocadas por esta metodologia e que, no seu conjunto, irão permitir o desenho funcional de um sistema de informação para gestão de risco operacional capaz de responder aos requisitos mais emergentes colocados às instituições financeiras. De seguida, são endereçadas as diferentes questões identificadas pela metodologia:

Qual é o problema real?

Criar um sistema de informação para a gestão de risco operacional que não só permita responder às entidades supervisoras (o Banco de Portugal e o Instituto de Seguros de Portugal reconhecem a importância da existência de um sistema de

informação para gestão de risco operacional), mas se traduza igualmente numa ferramenta essencial no processo de definição da estratégia e no controlo e acompanhamento da sua implementação, ou seja, que possibilite gerir (identificar, avaliar e mitigar) factores passíveis de implicar o falhanço da instituição em algum dos seus objectivos de performance operacional, tal como foi mostrado na definição de risco operacional apresentada em Vinella e Jin (2005). É necessário um sistema de informação que garanta que a instituição responde aos requisitos definidos pela supervisão, tanto na metodologia de cálculo de capital a alocar, quanto na forma como a apoia na implementação do seu processo de gestão de risco operacional. O reconhecimento do valor potencial da informação que estes sistemas podem fornecer à gestão das instituições impõe que os futuros sistemas de informação possuam funcionalidades que os elevem a ferramentas essenciais no processo de definição da estratégia, bem como nos processos diários de cada organização.

Quais são os objectivos a atingir, tendo em conta a percepção acerca da situação actual do problema?

1. O sistema deverá ter a capacidade de responder a todos os requisitos impostos pelas entidades supervisoras às instituições financeiras, qualquer que seja a abordagem que estas desejem seguir – este facto foi claramente referido, tanto por bancos quanto por seguradoras, como um dos principais objectivos dos seus programas de gestão de risco operacional. Torna-se pertinente enfatizar que a supervisão vai estar mais concentrada em aspectos relacionados com a forma como o sistema de informação influi no processo de gestão de risco operacional, do que na sofisticação das análises efectuadas (desde que estas cumpram os requisitos regulamentares). Aspectos como a capacidade da instituição para construir a sua base de dados de risco operacional, garantindo uma abrangência

e integridade (segregação de funções) que permitam captar o seu real perfil de risco; a forma como mecanismos de controlo e planos de mitigação são implementados e a metodologia através da qual a gestão de risco operacional é integrada nos seus processos de negócio, tudo isto deverá constar dos pontos principais da actividade de supervisão.

2. Como referido no ponto anterior, o sistema deve ter a capacidade de fornecer informação de gestão que faculte, às diferentes estruturas organizativas, compreender os níveis de risco a que estão expostas e quais as medidas de mitigação mais adequadas para cada tipo de fonte de risco operacional – esta capacidade está de acordo com os objectivos definidos internamente nas instituições e também como o que Kingsley et al. propuseram em 1998 para uma arquitectura de gestão de risco operacional. Este ponto é possivelmente um dos mais desafiantes para as instituições, dado que esta é uma área que historicamente tinha um âmbito circunscrito às actividades de apenas algumas direcções, como à de Auditoria Interna ou à de Qualidade. A gestão de risco operacional vai alargar estas actividades às linhas de negócios e a todas as direcções da instituição, colocando também nestas a responsabilidade de perceber e mitigar o risco operacional dos seus processos (com impacto directo nos níveis de capital a alocar a cada linha de negócio). Assim, o sistema de informação deverá ter capacidades que façam com que os dados e as análises sejam disponibilizados a todas estas áreas, num formato que estas possam utilizar e integrar nas suas actividades diárias. Outro conjunto de informação mais agregada (e.g. níveis de exposição, necessidades de capital) deverá ser disponibilizado aos órgãos de gestão da instituição, para o integrarem no seu processo de decisão estratégico. Também de acordo com os princípios da

supervisão, e como foi apresentado por Helbock e Wagner (2006), o sistema deverá fornecer relatórios ao mercado sobre o programa de risco operacional da instituição, de forma a assegurar transparência sobre o seu processo de gestão;

3. O sistema deve integrar ferramentas analíticas que lhe permitam tratar cada fonte de risco de forma independente, com o objectivo de fornecer à gestão indicadores, padrões e regras que lhe possibilitem responder de forma pro-activa aos desafios colocados por cada tipo de risco operacional. Como já foi apresentado, o risco operacional tem origem num conjunto vasto de fontes e pode imprimir impacto em diferentes processos. Como tal, cada risco apresenta as suas características, pelo que aplicar as mesmas abordagens a diferentes riscos seria um erro grave. Assim, revela-se necessária a existência de ferramentas que facilitem endereçar estas diferentes especificidades (Cruz 2002), tendo sempre como objectivo que as suas análises apresentem resultados que possam ajudar a instituição a mitigar os riscos a que está exposta. O sistema deverá ser, também, um instrumento para garantir um elevado grau de segurança das instituições face a eventos de risco, quer internos, quer externos. Estas ferramentas têm de estar de acordo com os requisitos do regulador (Basileia II 2002) – como, por exemplo, ser passíveis de auditoria –, e, por outro lado, devem responder às necessidades internas da instituição, mostrando-se capazes de fornecer informação num formato perceptível para utilizadores nas linhas de negócio (Dowd 2003);
4. De uma forma mais operacional, o sistema de informação deverá contribuir com informação que permita à instituição reduzir a frequência e a severidade das suas perdas, bem como os custos associados a controlos ineficientes ou à alocação de recursos para fazer face a eventos de risco operacional. Deverá representar

sempre um ponto central para os mecanismos de controlo interno da instituição, com o intuito de garantir que processos, riscos e controlos se encontram perfeitamente documentados e avaliados. Todo este processo irá contribuir para que a instituição melhore a forma como desenvolve as suas actividades, o que lhe permitirá garantir melhores condições de trabalho aos seus colaboradores e serviços mais eficientes para os seus clientes e outras entidades com as quais interactua.

5. Por fim, deve o sistema traduzir-se numa fonte consolidada de disseminação da cultura de risco operacional dentro da instituição – um dos principais desafios identificado pela maioria das instituições nas suas respostas ao questionário. Este processo de disseminação revelar-se-á crucial no envolvimento de toda a instituição em torno dos princípios fundamentais do seu programa de gestão de risco, garantindo uma maior adesão a processos como a recolha de dados ou o desenvolvimento de planos de mitigação. Também será essencial para assegurar que os processos e as actividades da instituição respeitam as normas gerais e específicas do mercado onde actua e que se mostram alinhados com os objectivos estratégicos da instituição.

Quais são os constrangimentos?

Os constrangimentos que o sistema terá de enfrentar derivam sobremaneira de este ser um tema novo no que concerne ao seu tratamento por parte das instituições financeiras (Raft International 2002). Como tal, não existe ainda um corpo de conhecimento ou experiência que possa ser um forte alicerce para estes desenvolvimentos, o que leva a que as instituições tentem aprender umas com as outras – em Portugal, algumas instituições bancárias reúnem-se periodicamente (aproximadamente, com uma periodicidade trimestral) para trocarem informações sobre

como estão a implementar os seus programas de gestão de risco operacional. Como foi apresentado no capítulo "Dados", a falta de informação, essencialmente quantitativa, é, e continuará a ser, um dos grandes obstáculos à implementação de sistemas de informação capazes de fornecer dados fiáveis e em tempo útil, além de acarretar um impacto directo sobre a selecção das metodologias de análise passíveis de utilização e sobre o real valor dos seus resultados. Outro constrangimento vem da abrangência implícita no risco operacional – o seu conceito tão alargado e a própria falta de concordância sobre uma definição padrão leva a que tenham de ser desenvolvidas áreas tão distintas como a falha de sistemas ou a fraude externa. Na apresentação dos desafios para os sistemas de informação para gestão de risco operacional, Netter e Poulsen (2003) incluem o desenho de modelos para cada uma das áreas específicas de risco, o que irá obrigar a desenvolvimentos extremamente distintivos e adaptativos, para os quais não existem, na maioria dos casos, dados e investigação académica que os suporte – esta situação obriga a um elevado número de recursos técnicos, humanos e financeiros por parte da instituição. Por último, o problema do entendimento do conceito de risco operacional, da sua gestão e mais-valias, será um constrangimento de ordem cultural que colocará problemas sérios à correcta implementação dos sistemas de informação (e.g. registo de eventos e construção de medidas de mitigação), alguns dos quais foram identificados por Currie (2004). Este ponto foi claramente reconhecido pela maioria das instituições como o seu maior desafio para o desenvolvimento de programas de gestão de risco operacional.

Quem são os intervenientes?

Os intervenientes neste sistema deverão ser todos os níveis da organização que possam desempenhar um papel relevante nos processos necessários para atingir os objectivos identificados para o programa de gestão de risco operacional. No entanto,

como pôde ser observado nas conclusões das entrevistas, as diferentes instituições têm abordagens diferentes sobre a difusão do sistema ao longo da organização, apesar de haver uma tendência explícita para a expansão do sistema de informação a um número cada vez maior de utilizadores. Existem já instituições que se encontram a expandir a utilização destes sistemas às direcções de Auditoria Interna e *Compliance*, pois são duas entidades que partilham uma base comum de informação, análises e relatórios – será um erro grave que estas duas direcções e a de gestão de risco operacional usarem diferentes fontes de informação, pois isso irá certamente provocar situações de falta de integridade e de inconsistência entre os resultados apresentados por cada uma delas. Espera-se, no futuro, que outros departamentos mais operacionais venham também a ter uma intervenção elevada, do qual são exemplos os departamentos de desenvolvimento de produtos, o departamento de sistemas de informação, o departamento comercial, o departamento financeiro e todos aqueles que possam, de uma forma ou de outra, estar ligados a processos susceptíveis de trazer ou mitigar risco operacional nas instituições financeiras (até à data, o contributo destas direcções resume-se à recolha de eventos ou à resposta a questionários de auto-avaliação) – se existir uma visão alargada, o grupo de departamentos intervenientes poderá confundir-se com a totalidade da instituição. Todo este processo de expansão da gestão de risco operacional dentro das instituições torna ainda mais primordial a resolução do desafio cultural já anteriormente mencionado, pois só com a sua resolução o processo de expansão poderá ter sucesso.

Quem são os beneficiários?

1. A instituição financeira – mediante um sistema de informação bem desenhado, pode conseguir melhorar os seus níveis de gestão qualitativos e quantitativos, através quer do aumento do conhecimento sobre os seus processos, quer da redução das suas perdas, dos seus custos operacionais e da sua exposição a

eventos internos e externos. Todos estes pontos irão permitir que as instituições que sigam as abordagens avançadas do supervisor aloquem menos capital para risco operacional; garantem, igualmente, uma melhor imagem perante o supervisor e o mercado através de processos mais transparentes, melhores produtos e serviços de qualidade superior. Estas conclusões são sustentadas pelas mais-valias identificadas pelas diferentes instituições na resposta ao questionário (Figura 14 – Mais-valias da gestão de risco operacional para a banca; Figura 22 – Mais-valias da gestão de risco operacional para as seguradoras);

2. Os accionistas – que vêem, desta forma, a instituição na qual investiram mais fortalecida em dois vectores: na sua capacidade de fazer face a eventos de risco operacional e de os prever ou mitigar, bem como na imagem que a empresa passa a ter no mercado, tal como foi proposto por Helbok e Wagner (2006). Todos estes pontos são fortes indicadores de uma instituição capaz de construir valor para aqueles que nela investem; reduzem, igualmente, a necessidade de os accionistas terem de proceder a aumentos de capital com vista a responder a requisitos do supervisor para fazer face à exposição da instituição a risco operacional;
3. O cliente – se a instituição fizer uma correcta e eficiente gestão de risco operacional, será expectável que a qualidade dos seus produtos e serviços comporte uma melhoria considerável (aspecto encarado por algumas instituições financeiras como um dos objectivos dos seus programas de gestão de risco operacional). O autor não teve acesso a estudos que sustentem esta conclusão, no entanto, uma melhor gestão de risco operacional deverá exercer um impacto directo sobre a redução dos erros nos processos que envolvem o cliente

(melhoria da qualidade do serviço prestado), além de que poderá significar mesmo uma redução dos custos em produtos e serviços prestados, devido à diminuição das perdas associadas a eventos e à utilização mais proveitosa dos controlos internos e outras medidas de mitigação. Este ponto pode vir a incutir um impacto directo sobre o preço aplicado pela instituição aos seus clientes;

4. O sistema financeiro – sendo estes sectores (especialmente a banca) extremamente contagiáveis, poder-se-á dizer que a segurança de uma instituição é também a segurança de todas as outras. O papel dos supervisores tem aqui o seu carácter mais exigente, no sentido de garantir a correcta aplicação de normas e directivas por parte de todas as instituições. O autor defende que, ao contrário do que Lewis e Lantsman (2005) apresentam, os eventos de risco operacional podem ter um efeito contagiante noutras instituições, quer através do impacto na imagem do sector, quer pelo facto de que, quando sucedem numa instituição, alguns tipos de eventos (e.g. fraude, quebras de sistemas) tendem a replicar-se noutras. No caso das seguradoras, a gestão de risco operacional, ao ajudar a garantir a sua solvabilidade, está a acautelar que estas instituições não entram em incumprimento, caso os seus clientes necessitem de accionar as cláusulas dos seus contractos;
5. O mercado – a crise financeira do final do ano de 2008 veio provar que as crises neste sector repercutem sempre elevados impactos em todos os sectores económicos. A dependência que praticamente toda a economia tem deste sector para o seu financiamento, para a poupança, investimentos e financiamento do risco (e.g. seguros) justifica este comportamento. A gestão de risco operacional, ao garantir a segurança e o correcto funcionamento de uma instituição financeira, está também a defender a solidez do sistema financeiro, assegurando,

assim, que os diferentes agentes económicos, sejam empresas, sejam particulares, tenham acesso a meios vitais (financiamento, meios de pagamento, seguros) às suas actividades diárias.

Quem são os reguladores?

Os reguladores do sistema deverão ser, numa primeira fase, os órgãos internos de controlo e auditoria das instituições, que terão a capacidade e a autonomia para regular e controlar o funcionamento do sistema no seu todo. A sua actuação seguirá princípios rigorosos de segregação de funções de forma a garantir uma total transparência no processo, o que deverá servir como factor-chave na apresentação do sistema de risco operacional como uma ferramenta global, cujo objectivo é a melhoria dos processos dentro da instituição, e não um sistema de controlo de erros ou repressão. O sistema de informação deve difundir o conceito de gestão de risco operacional como uma forte mais-valia para a instituição e para os seus colaboradores. Numa segunda fase, deverão ser os auditores externos das instituições (no âmbito dos seus processos de certificação) a avaliar a adequação e a fiabilidade do sistema implementado – este processo será importante para certificar o programa de risco operacional e o seu sistema de informação perante os diferentes agentes económicos. Na última fase, caberá aos órgãos supervisores (Bdp e ISP) auditar as instituições para garantir que estas estão de acordo com os normativos; que gerem o seu risco operacional de forma eficiente; que estão a alocar capital e que têm em prática as medidas de controlo e mitigação adequadas aos níveis de risco a que estão expostas.

Qual é o sistema e quais os ambientes envolvidos?

O desenho funcional do sistema de informação apresentado (Figura 25 – Diagrama do sistema de informação para gestão de risco operacional proposto pelo autor) tem como finalidade responder não só aos objectivos que foram identificados – a partir tanto

da revisão da literatura, quanto dos resultados obtidos nas entrevistas –, minimizando os impactos dos diferentes constrangimentos, como também a todos os requisitos dos diferentes intervenientes e supervisores. O sistema deverá ser composto por quatro ambientes principais, a saber: um primeiro ambiente, mais operacional, responsável pela interacção com os utilizadores ao nível da recolha de dados de eventos, questionários de auto-avaliação, testes aos controlos e outros conjuntos de informação cuja intervenção dos utilizadores seja necessária; o segundo, responsável por todo o acesso e carregamento de dados de forma automática, dos e para os sistemas operacionais (e.g. mapeamento de processos, riscos e controlos, KRI's, eventos registados noutros sistemas), e por todos os processos de integração com outros sistemas (e.g. reconciliação contabilística); o terceiro, mais analítico, é o responsável pelas análises mais específicas como, por exemplo, análises de custeio, estatísticas, padrões e comportamentos (probabilidade e impacto) de factores de risco, bem como pelos cálculos de capital e análise ao impacto das medidas de mitigação, incluindo análises aos controlos internos; o quarto é responsável por todas as funcionalidades de disponibilização de relatórios a todos os intervenientes e reguladores no processo de gestão de risco operacional e pelas análises de performance aplicadas a processos, linhas de negócio ou a outras dimensões onde se possam aplicar.

Como vai o sistema realizar as suas funções?

Um sistema de informação para gestão de risco operacional tem que ter uma representação bastante fiável do ambiente organizacional aonde vai operar, ou seja, numa primeira fase, o sistema terá de mapear o conhecimento interno da instituição sobre risco operacional; será, por outras palavras, o suporte para o conhecimento que a organização já possui relativo a processos, tipos de riscos operacionais, organização interna, causas de risco, medidas de mitigação, indicadores de risco, entre outros. O

sistema irá conter processos para aceder a todas as fontes de informação disponíveis, que encerrem dados relevantes para a gestão de risco operacional, e carregar a informação na base de dados, cumprindo, assim, os objectivos que Mestchian (2003) apontou para uma base de dados de risco operacional. Para os dados que não existem em suporte informático, o sistema irá disponibilizar interfaces gráficos para a recolha de dados de eventos, questionários de auto-avaliação, testes aos controlos e indicadores de risco – funcionalidades base requeridas pela maioria das instituições, por serem também as reclamadas pelos órgãos de supervisão. A informação pode ser obtida, igualmente, através do sistema de alocação de custos para enriquecer a base de dados de risco operacional com dados referentes a custos indirectos, tal como foi proposto por Mestchian (2003). Toda a informação poderá ser, então, tratada por dois subsistemas: (i) um para cálculo de requisitos de capital, permitindo, assim, à instituição responder aos requisitos da abordagem regulamentar a que resolver candidatar-se e alocar capital a linhas de negócio de acordo com o seu perfil de risco; (ii) outro para a análise mais detalhada de cada tipo de risco operacional, tentando identificar factores de risco, tendências, comportamentos e padrões, fornecendo à instituição mais conhecimento que lhe permita prever e mitigar os riscos mais críticos. Com base nesta informação, o subsistema de mitigação pode ser utilizado para o lançamento e acompanhamento de diversas medidas com o objectivo de gerir os níveis de exposição a risco operacional da instituição. Este subsistema também deverá ser responsável pelo acompanhamento da implementação e eficácia dos controlos internos. Toda a informação recolhida e tratada pode ser utilizada para a análise de performance das diferentes dimensões, para a produção de relatórios destinados às entidades supervisoras, bem como para a disponibilização de indicadores de gestão a toda a instituição. Outro processo que também poderá e deverá ser implementado passa pelo carregamento dos sistemas

operacionais da instituição com os dados produzidos pelo sistema de risco operacional, permitindo, deste modo, que os diferentes níveis da organização possam utilizar este conhecimento nas suas actividades diárias; possibilitando, inclusive, que a cultura de risco operacional seja mais bem assimilada por toda a organização.

Em conjunto, estes subsistemas irão conseguir: (i) atingir os objectivos de gestão, como os apresentados por Netter e Poulsen (2003); (ii) responder aos requisitos dos supervisores (Basileia II 2002) e (iii) corresponder às expectativas que instituições financeiras depositam nos seus sistemas de informação (Figura 9 – Objectivos da gestão de risco operacional na banca; Figura 17 – Objectivos da gestão de risco operacional nas seguradoras).

Quais os seus subsistemas?

O conjunto de subsistemas que é proposto poderá ser disponibilizado da forma como é apresentado, ou desenvolvido em diferentes arquitecturas, ou níveis, de acordo com a capacidade e recursos humanos, técnicos e financeiros da instituição, em concerto com os seus objectivos específicos para o programa de risco operacional. É igualmente expectável que, na sua quase totalidade, as instituições não optem, numa primeira fase, pela implementação completa da arquitectura do sistema de informação, preferindo ir evoluindo o sistema por etapas, segmentando recursos e utilizando o conhecimento adquirido em cada uma das etapas para melhorar o processo de implementação nas seguintes. Possivelmente, a maior vantagem desta abordagem faseada é o proporcionar do desenvolvimento da cultura de risco operacional de uma forma sustentada, sem criar "pontos de fricção" nos processos de negócio diários da instituição. O autor apresenta uma arquitectura constituída por sete subsistemas, nomeadamente:

1. Sistema de acesso a fontes de dados (os dados que são alvo de tratamento neste sistema são os mencionados no capítulo 3.1 – Dados) – este subsistema é

responsável por duas funções primárias fundamentais, que foram claramente identificadas pelas instituições financeiras, enquanto as principais que deverão existir nos seus sistemas de informação: a primeira é garantir que todos os dados relevantes para o sistema de gestão de risco operacional são recolhidos dos diferentes sistemas operacionais da instituição. Para tal, o sistema deve ter a capacidade de acesso a diferentes fontes e estruturas de dados (não é comum que uma instituição utilize um só fornecedor de base de dados); deve, também, possuir mecanismos que permitam afiançar que este processo de integração é realizado dentro de objectivos elevados de qualidade e validade dos dados, integrando os diversos conceitos de negócio existentes. A segunda das mencionadas funções primárias passa por disponibilizar um interface gráfico que permita registar eventos, auto-avaliações, indicadores, cenários e testes aos controlos, ou seja, todo o conjunto de dados que não se encontram registados em nenhum suporte electrónico passível de ser acedido pelo sistema. O desenho deste interface gráfico deve considerar dois aspectos críticos para garantir o seu sucesso: a facilidade da sua utilização, de forma a mitigar os riscos culturais inerentes ao próprio processo de registo de informação de risco operacional, e a concordância com políticas de segregação de funções, que assevere que o sistema opera dentro dos requisitos impostos pelo supervisor. Uma terceira função, ainda não identificada de uma forma directa pelas instituições, mas pela qual este subsistema também é responsável, é o carregamento dos resultados das diferentes análises de risco operacional nos sistemas operacionais da instituição financeira – só desta forma, poderão as áreas mais operacionais da instituição utilizar e aplicar informação de gestão de risco operacional nas suas actividades e processos diários, potenciando a criação de valor baseada na gestão de risco

operacional. Neste ponto, o aspecto mais relevante a ter em atenção é a forma e o conteúdo com que esta informação deve ser integrada para que seja facilmente entendida pelas diferentes áreas;

2. Sistema de cálculo e alocação de capital – apesar das respostas aos questionários terem revelado que o cálculo de requisitos de capital não representa, presentemente, uma das principais preocupações das instituições financeiras portuguesas, a existência deste subsistema justifica-se pelo facto de potenciar nas instituições o desenvolvimento de meios para realizar todos os cálculos e análises requeridos no âmbito da actividade de supervisão (Basileia II 2002). Deverá também contemplar todo o conjunto de outros cálculos de capital que a instituição considere necessários à sua actividade de gestão de risco operacional, tais como a análise do impacto das medidas de mitigação no capital, a análise de correlação entre diferentes tipos de riscos, ou cálculo do capital económico para risco operacional segundo diferentes abordagens, ao encontro da proposta de Dowd (2003). Outra capacidade fundamental equivale à alocação de capital aos diversos níveis da instituição (e.g. linhas de negócio, categoria de risco). Se uma instituição financeira pretender alargar a sua actividade de risco operacional a outras dimensões e calcular o seu consumo de capital para risco operacional por processo, produto ou departamento, têm de haver mecanismos que permitam a alocação de capital a estas dimensões. Existem diversas metodologias disponíveis para alcançar este objectivo (Marshall 2001), sendo os indicadores de gestão umas das mais utilizadas para a sua concretização;
3. Sistema analítico de risco operacional – a etiologia do risco operacional advém de diferentes fontes, algumas delas de difícil modelação pelas técnicas tradicionais. Embora este requisito não haja sido claramente identificado nas

respostas ao questionário, a literatura veicula fortes argumentos que indicam que, se uma instituição financeira quiser elevar o nível da qualidade da sua gestão de risco operacional, terá de possuir sistemas que lhe permitam analisar e modelar os seus principais riscos operacionais de forma isolada e sistemática, sejam eles as falhas de sistemas, erros em processos, ou as fraudes, como o propuseram Netter e Poulsen (2003). Os modelos utilizados para a análise destes tipos de risco têm que ter características únicas, uma vez que, na maioria dos casos, os dados a tratar têm por base comportamentos humanos e estes qualificam-se, por seu lado, pela sua natureza adaptativa e influenciável – e, por isso mesmo, de difícil modelação – tal como foi identificado por Marshall (2001). No entanto, se este subsistema possuir ferramentas analíticas avançadas – tais como redes neuronais, árvores de decisão, ou *fuzzy logic*, entre outras –, há já evidências teóricas e práticas de que este tipo de sistemas pode auxiliar na detecção e mitigação de eventos de risco operacional, como o elucidou Cruz (2002). Munidas deste conhecimento, as instituições financeiras poderão utilizá-lo para desenvolver e melhorar os seus controlos internos e outras medidas de mitigação. Este subsistema também deverá ter a capacidade de realizar análises de séries temporais, para fornecer à gestão conhecimento sobre tendências cíclicas dos seus eventos ou tipos de risco, e análises de previsão, para que a instituição possa alocar os seus recursos de acordo com as necessidades identificadas;

4. Sistema de mitigação – a mitigação de risco é um processo fundamental na gestão de risco operacional. Assim, é necessário que os sistemas de informação das instituições financeiras tenham ferramentas que as ajudem a implementar as diferentes medidas de mitigação que pretendam desenvolver. Este subsistema

deve permitir analisar medidas de mitigação não só reactivas, como as apólices de seguros, mas também pró-activas, como planos de formação ou reestruturação de processos. Deverá ter a capacidade de avaliar os impactos dos diferentes controlos internos activos na organização – ou seja, o seu custo e capacidade de detecção de eventos de risco –, através, por exemplo, da utilização de métricas como o risco líquido ou o residual como indicador da capacidade dos controlos para mitigarem os riscos a que se encontram associados. Independentemente das medidas de mitigação que a instituição decida aplicar, este subsistema deve ter a capacidade para definir a medida de mitigação (incluindo custo e potencial de melhoria), acompanhar a aplicação das diferentes medidas e avaliar o real impacto da aplicação de cada medida de mitigação na redução da frequência e/ou severidade dos eventos para os quais foi desenvolvida;

5. Sistema de cálculo e afectação de custos – este subsistema é dos mais difíceis de implementar. Tem por objectivo o cálculo de dois tipos de dados para alimentar o sistema global de gestão de risco operacional. Tal como foi demonstrado por Haas e Kaiser (2004), existem muitas instituições financeiras que conseguem ter informação sobre a frequência com que determinado tipo de evento ocorre, mas têm grande dificuldade em associar um valor à severidade. Assim, o primeiro tipo de dados a ser calculado refere-se à estimativa para a severidade destes eventos. Este valor pode ser calculado utilizando diferentes metodologias, de entre as quais se destacam os modelos baseados no cálculo de métricas estatísticas simples – recorrendo a eventos passados em questionários de auto-avaliação, ou a métodos estocásticos, em modelos mais complexos (e.g. teoria de ruína, *realiability theory*), como foi apontado por Cruz (2002). A

reconciliação contabilística também poderá ser utilizada para inferir o valor de severidade de alguns eventos, pois fornece informação dos valores que foram registados, associados a determinados eventos, que podem ser uma boa *proxy* para o valor da severidade dos novos eventos. O segundo tipo de dados refere-se a custos indirectos, como proposto por Mestchian (2003). A gestão de risco operacional tem vindo a ser realizada, tendo fundamentalmente por base a utilização dos custos directos no cálculo da severidade. No entanto, já é reconhecida a importância e o impacto nas instituições financeiras dos custos indirectos de certos tipos de risco. Uma das principais razões que dificulta a sua utilização é a complexidade inerente ao cálculo de alguns dos custos indirectos como, por exemplo, a perda de quota de mercado ou de reputação. É possível endereçar estes problemas através da incorporação, nos sistemas de risco operacional, de sistemas de *Activity Based Management* (ABM). Estes sistemas permitem associar proveitos e custos a diferentes dimensões, com base em distintos critérios, estabelecendo, assim, regras para associar eventos a perdas de receita ou a custos indirectos. Com o recurso a sistemas de ABM, poder-se-á utilizar o valor de proveitos calculado para uma actividade e aplicá-lo ao cálculo da severidade esperada de um evento, passando esta severidade a ser a soma entre o valor de perda directa do evento e o valor dos proveitos esperados nas actividades que foram afectadas para ocorrência do evento. A utilização de sistemas de ABM pode ser também levada à prática para associar à severidade de um evento os custos de actividades que vão ser afectados pela sua ocorrência. Por exemplo, eventos que, após a sua ocorrência, impliquem que algumas actividades sejam extraordinariamente executadas para que a instituição consiga continuar a operar no seu nível de serviço habitual devem incluir no cálculo da

sua severidade não só a perda directa, mas também os custos indirectos decorrentes da utilização de actividades de manutenção e controlo, ou custos associados à necessidade de mais recursos para as actividades afectadas (e.g. horas extraordinárias). Não existe ainda uma metodologia consistente para aplicar a esta associação entre eventos, proveitos e custos. Em todo o caso, o autor sugere que, numa fase inicial, o critério da proporcionalidade seja aplicado, utilizando métricas como o volume de negócios ou o número de recursos alocados de cada actividade afectada pelo evento;

6. Sistema de análise de performance – apesar de já em 1997 Gibson ter apontado a necessidade de usar o risco na análise da performance, a utilização do risco operacional como uma das bases para a avaliação de desempenho nas instituições financeiras não é comum. Esta situação deriva da dificuldade que ainda hoje existe nos cálculos deste tipo de risco e, numa fase seguinte, na alocação dos resultados aos diferentes níveis da instituição para que estes entrem nos indicadores de performance. É expectável, no entanto, que algumas das instituições venham a desenvolver este tipo de análise para algumas das suas dimensões como, por exemplo, linha de negócio, produto, departamento ou processo. A informação de frequência e severidade, dados de diferentes indicadores de gestão e dados de controlo interno podem permitir aplicar análises de performance baseadas na exposição a risco operacional e na capacidade da sua gestão. Existe informação nos sistemas de gestão de risco operacional passível de ser aplicada para análise à performance da instituição, das suas áreas de negócio, ou mesmo dos seus colaboradores. Por exemplo, o número de eventos e sua severidade, ponderados pelo volume de clientes ou operações, pode ser um indicador a incorporar na avaliação de um departamento,

como um parâmetro da sua qualidade de gestão. Outros exemplos são: a análise à eficácia e eficiência dos controlos existentes – este critério avalia a performance relativa à capacidade para executar os controlos de acordo com as suas especificações e garantindo os objectivos para os quais foram desenhados; a aplicação com sucesso das medidas de mitigação – este critério irá permitir avaliar a capacidade das diferentes áreas da instituição para aplicar as medidas de mitigação pré-estabelecidas, ou para desenvolver novas medidas como forma de reagir a novas fontes de risco operacional. Utilizados isoladamente, ou em conjunto, estes indicadores irão permitir uma avaliação baseada não só em resultados financeiros, mas também em critérios associados à qualidade do processo de gestão, tais como: a capacidade de executar o processo com um número mínimo de erros; a execução de controlos com alto nível de eficácia ou a aplicação de medidas de mitigação com elevado sucesso. A combinação entre os resultados financeiros e a qualidade da gestão (elevado nível na gestão de risco operacional) deverá servir como base para a criação de uma métrica a utilizar para avaliar direcções, linhas de negócio e, quando possível, colaboradores;

7. Sistema de reporte – a premissa base que justifica a necessidade de uma componente de reporte robusta dentro do sistema de informação foi apresentada no capítulo 3.3 – Relatórios – e igualmente identificada pelas instituições nas suas respostas ao questionário. Este subsistema deverá ter dois objectivos fundamentais: em primeiro lugar, (i) a produção de todo o reporte solicitado pelas entidades supervisoras – facto claramente mencionado pelas instituições nas suas respostas ao questionário. Esta informação, requerida através de ficheiros de dados, relatórios tabulares ou gráficos, deve ser produzida por um processo que seja o mais automático possível e em períodos de tempo que

permitam responder, sem qualquer constrangimento, aos requisitos regulamentares. É também necessário garantir a flexibilidade na produção destes relatórios, pois existe a possibilidade de o supervisor alterar os seus requisitos, bem como requerer à instituição a disponibilização de outro conjunto de dados, de acordo com as conclusões que vai obtendo durante o processo de supervisão. Em segundo lugar está (ii) a disponibilização de toda a informação solicitada pelos diversos níveis da organização, para que estes fiquem capacitados com todo o conhecimento necessário para incorporar os conceitos de gestão de risco operacional nas suas actividades. Estes relatórios também irão desempenhar um papel fundamental para o desenvolvimento dos conceitos e metodologias de risco operacional dentro da instituição. Para o apoiar nestes dois objectivos cimeiros, o sistema deve contemplar ferramentas que permitam, a cada utilizador, elaborar, de forma autónoma, os relatórios que se traduzam necessários para a condução das suas actividades e a concretização dos seus objectivos – para tal, há que garantir que a informação a que o utilizador tem acesso não só é actual e fiável, como está em concerto com as políticas de acesso a dados da instituição.

Quais deverão ser os critérios de avaliação do sistema?

O sistema de informação deve ser avaliado de acordo com os objectivos para os quais foi concebido, incluindo as mais-valias (directas e indirectas) e os custos (financeiros e de recursos) associados à sua implementação. De seguida, apresentam-se alguns dos critérios passíveis de utilizar nesta avaliação, embora cada organização deva estabelecer internamente qual o melhor método para avaliar as capacidades e a adequação do seu sistema de informação:

1. Capacidade de responder aos requisitos do regulador – o sistema de informação deverá ter a capacidade de responder aos requisitos de supervisão que se apliquem na sua área de actuação – em Portugal, as normas do BdP ou do ISP. Esta resposta deve ter em conta métricas, estrutura e formato da informação a disponibilizar, bem como os prazos a cumprir – para estes, o sistema deve permitir a parametrização de um conjunto de alertas que apoiem a instituição no seu cumprimento. Um aspecto essencial na avaliação do supervisor é o requisito referente ao próprio processo e estrutura do programa de gestão de risco operacional da instituição, mais especificamente sobre o funcionamento do sistema de informação – a existência de *workflows* de aprovação de dados e o nível de segregação de funções existente no sistema de informação perfazem factores claramente avaliados pelo supervisor. Apesar de o Acordo de Basileia II impor regras para a uniformização dos requisitos dos diferentes supervisores, as instituições com representação em múltiplas zonas geográficas devem ter em atenção as possíveis especificidades que cada legislação local lhes possa exigir – um factor a considerar num sistema de informação é a sua facilidade para se adaptar a legislação e requisitos novos que surjam por parte do regulador;
2. Redução de perdas e custos operacionais – este constituiu um dos objectivos primários para a banca, no contexto do seu programa de gestão de risco operacional, e uma das mais-valias identificadas pelas seguradoras. Este critério pode ser directamente utilizado para avaliar o sistema de informação para gestão de risco operacional e a sua capacidade de criar conhecimento que a instituição possa utilizar para desenvolver planos de mitigação, ou melhor, os seus processos de negócio – se bem desenvolvidas, estas duas medidas irão permitir à instituição reduzir as suas perdas e custos operacionais. O sistema pode ser

avaliado através da análise directa da frequência e severidade das perdas, através da consulta às contas de custos operacionais, ou pelo número de vezes que certas medidas de mitigação são accionadas (e.g. apólices de seguros – a sua activação está associada à ocorrência de eventos).

3. Eficácia dos controlos internos e das medidas de mitigação – este critério está directamente relacionado com o anterior, porque se refere à capacidade da instituição para implementar mecanismos de controlo interno a fim de detectar e evitar perdas potenciais, bem como para o desenvolvimento de medidas de mitigação que melhorem processos ou reduzam a severidade dos eventos. Assim, a avaliação deste critério divide-se entre a utilização racional dos controlos e medidas de mitigação e a sua capacidade para reduzir a frequência e/ou severidade de eventos. O sistema de informação deve ser avaliado com base na eficácia dos controlos internos que analisa e acompanha. Este critério está ligado à capacidade da instituição de recolher informação associada aos seus controlos e implementar medidas que incrementem as capacidades desses mecanismos para reduzir a sua exposição a risco operacional. Relativamente às medidas de mitigação, o sistema pode ser avaliado pela sua capacidade para identificar essas medidas e dar informação para que elas sejam implementadas com maior sucesso, devendo disponibilizar informação sobre o custo e níveis de melhoria alcançados pelas diferentes medidas de mitigação;
4. Melhoria na qualidade de produtos e serviços – um dos critérios que também poderá ser utilizado para avaliar o sistema de informação tem por base a análise do impacto da gestão de risco operacional na melhoria da qualidade dos produtos e serviços da instituição financeira (identificado por algumas das instituições nas suas respostas). A grande dificuldade neste critério reside em

concretizar uma correlação entre a gestão do risco operacional e estas melhorias, já que estas podem estar ligadas a muitos outros factores. No entanto, nem que seja baseada em conceitos teóricos, ou em melhores práticas, é bastante expectável que uma boa gestão de risco operacional traga melhorias significativas na relação com os clientes, através do incremento da qualidade quer dos produtos oferecidos, quer dos serviços prestados. Alguns indicadores de risco podem ser utilizados para que a instituição logre compreender a evolução desta potencial melhoria, tais como o número de reclamações feitas por clientes, o número de casos de fraude que tiveram sucesso, a diminuição dos custos de manutenção, a rotação não planeada de colaboradores e a redução de número de falhas no processamento de operações. A alocação de pontos de controlo interno e a implementação de medidas de mitigação para estes indicadores irão ter impacto directo sobre a qualidade dos produtos oferecidos e serviços prestados pelas instituições;

5. Melhoria da cultura de risco – outro critério de avaliação indirecto é a melhoria da percepção de risco operacional por parte de todos os níveis e colaboradores da instituição – principal mais-valia, e desafio, identificada pela quase totalidade das instituições de ambos os sectores. A adesão das diferentes áreas dentro da instituição a processos de gestão de risco operacional, como, por exemplo, à recolha de eventos ou à resposta a questionários de avaliação de riscos, é o resultado directo da sua capacidade de absorção dos conceitos e metodologias de gestão de risco operacional. Também a capacidade de todos os níveis em incorporar nas suas actividades e processos diários conceitos como exposição ao risco, causas, tipos de risco, medidas de mitigação, entre outros, é uma clara

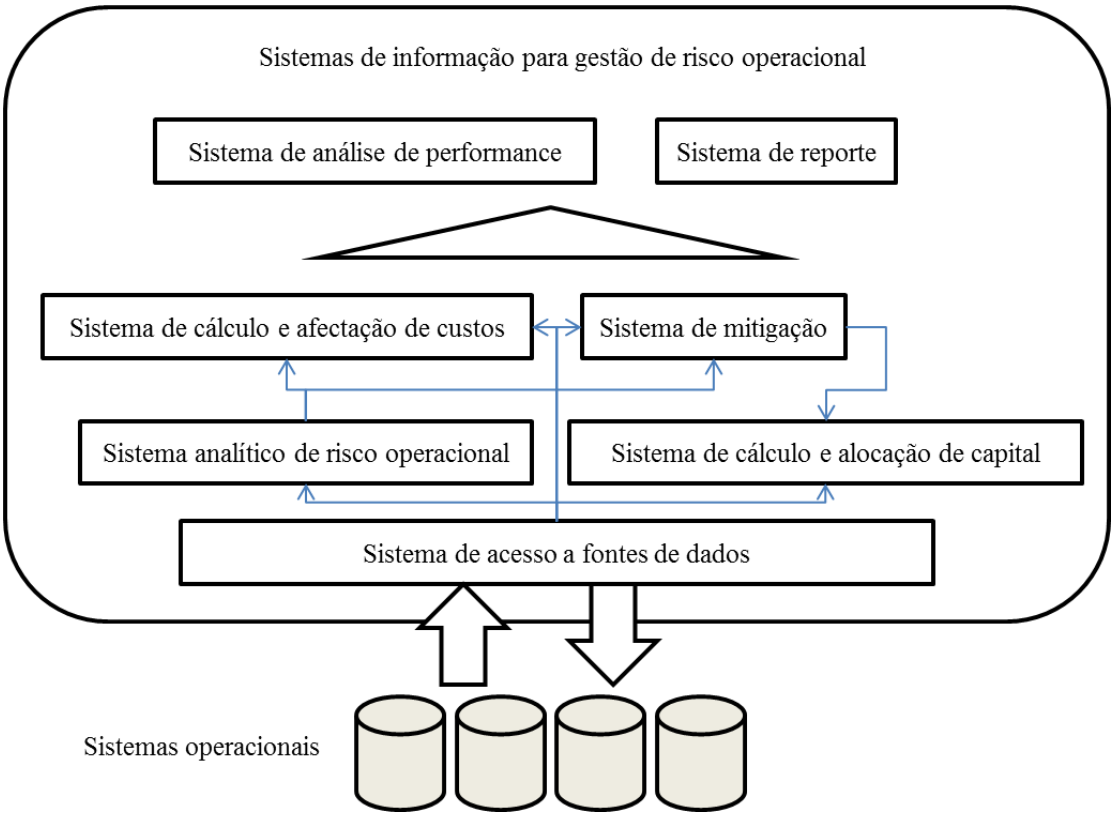
demonstração da qualidade do sistema de informação em disseminar a cultura de risco operacional;

6. Melhoria de imagem para o mercado e para os investidores – um critério que também não é de fácil quantificação, embora se revista de enorme importância para as instituições financeiras, uma vez que é a qualidade e o valor da sua imagem para o mercado e para os investidores. A imagem que o mercado tem da qualidade da gestão de risco operacional de uma instituição, já estudada e demonstrada por Helbok e Wagner (2006) e por Watts e Zimmerman (1986), é uma forte garantia de estabilidade e segurança e, consequentemente, um indicador para a confiança por parte dos clientes. Também é expectável que os investidores exijam taxas de retorno menos elevadas de instituições que apresentem menor risco. Já as empresas de *rating* irão avaliar a qualidade da gestão de risco operacional e do seu sistema de informação no momento em que concedem a sua classificação às instituições financeiras. Por fim, e ao abrigo do pilar II do Acordo de Basileia II, os supervisores irão certificar as instituições no que concerne à qualidade da execução dos processos de gestão de risco operacional, bem como do sistema de informação que lhe dá suporte. Será também pedido às instituições que forneçam ao mercado um conjunto de informação relativa aos seus níveis de exposição e risco operacional e a como está estruturado o seu programa de gestão deste risco – pilar III do Acordo Basileia II, o que contribuirá significativamente para a criação de uma imagem de solidez, ou fraqueza, da instituição perante o mercado.

O sistema de gestão de risco operacional deve ser sempre uma ferramenta fundamental no processo de gestão de uma instituição financeira. Por conseguinte, deve

ser flexível para se adequar às estratégias definidas e ter a capacidade de se integrar dentro das actividades e processos operacionais, para que apoie a instituição no seu desenvolvimento sustentado, através quer da melhoria dos seus resultados, quer da redução das suas perdas. Talvez o seu potencial mais significativo resida na sua capacidade para ser um forte mecanismo de disseminação do programa de gestão de risco operacional e, assim, um factor de mudança de comportamentos, abordagens de gestão e mesmo de alteração de estratégias. No entanto, o sistema de informação pode também ser ele próprio um factor de risco, pois uma má implementação pode criar barreiras à sua utilização, contribuindo ainda mais para que os seus objectivos sejam mal compreendidos e os seus resultados erradamente interpretados. O sucesso desta implementação passa, na maioria dos casos, por um processo evolutivo e pela capacidade da instituição para alocar recursos e envolver o máximo da organização em torno do seu programa de risco operacional. Neste processo evolutivo, será de esperar que as instituições desenvolvam primeiro os módulos específicos para responder aos requisitos do supervisor e do mercado (e.g. empresas de *rating*). Nas iterações seguintes, as instituições irão procurar implementar funcionalidades que lhes permitam recolher mais dados para enriquecer as suas análises e criar conhecimento para as ajudar a enfrentar desafios, a diminuir fragilidades, a melhorar as suas actividades, a aumentar a sua rentabilidade e a elevar o seu valor perante os seus colaboradores, clientes, accionistas, supervisores e mercado em geral. No caso de a implementação ser bem sucedida, o conhecimento que o sistema tem capacidade de produzir tornar-se-á potencialmente num factor crítico no sucesso de uma instituição financeira, não só através da garantia da sua sobrevivência, mas também pela capacidade de a distinguir em qualidade e "valor" das outras instituições.

Figura 25 – Diagrama do sistema de informação para gestão de risco operacional proposto pelo autor



VI PARTE – CONCLUSÕES E INVESTIGAÇÃO FUTURA

7 – CONCLUSÕES

Apesar de só nos últimos anos o risco operacional ter começado a ser alvo de regulamentação, de estudos académicos e de programas estruturados de gestão dentro das instituições financeiras, o reconhecimento da sua importância e do seu impacto é um facto incontornável. Esta situação pode ser comprovada através de estudos realizados no sector financeiro (Enterprise risk management in Financial service organizations 2008), de estudos académicos, como os de Cummings et al. (2006) e Wei (2006), de inúmeros casos que surgiram a público sobre instituições financeiras que sofreram elevadas perdas derivadas de factores ligados ao risco operacional (e.g. Societe Generale), bem como através do número crescente de implementações de programas e sistemas de informação em instituições financeiras.

O risco operacional em instituições financeiras tem um impacto mais elevado devido ao carácter sistémico de todo este sector económico, obrigando, em situações de crise, os governos centrais de diversos países a ter de actuar, através quer da concessão de garantias para empréstimos, quer mesmo da entrada, hostil ou não, no capital de algumas instituições. Um conjunto diverso de regulamentação já foi posto em prática (Basileia II), ou irá ser posto num futuro próximo (Solvência II), de forma a incentivar as instituições financeiras a melhorarem os seus processos de gestão de risco operacional e a criarem meios que facilitem às entidades de supervisão as suas tarefas de controlo do sistema financeiro. No entanto, uma das críticas a este conjunto de regulamentação é a de que o legislador centrou a sua atenção mais nos requisitos de cálculo de capital de risco operacional e menos no fomento do desenvolvimento de arquitecturas para assegurar uma eficiente gestão de risco operacional dentro das instituições, tal como foi proposto por Kingsley, et al. (1998) ou por Netter e Poulsen

(2003). Mesmo no tocante às abordagens de cálculo de capital propostas pelo Acordo Basileia II, autores como Moosa (2008) ou Kalhoff e Hass (2004) apresentam fortes críticas relativamente às reais vantagens das abordagens avançadas do Acordo e sobre a mais-valia de ser uma melhor metodologia para captar o real perfil de cada instituição.

Embora se deva, em grande parte, às pressões regulamentares, também na literatura se podem encontrar diversos factores que contribuíram para o desenvolvimento de gestão de risco operacional em instituições financeiras, tais como a redução de perdas e custos ou a melhoria dos processos de controlo interno. Tendo por base a definição de risco operacional apresentada por Vinella e Jin (2005), a gestão de risco operacional deverá debruçar-se sobre todos os factores que possam afectar a concretização dos objectivos da instituição, sejam quantitativos, associados a proveitos ou custos, sejam qualitativos, como a melhoria da reputação da instituição ou de indicadores de sustentabilidade. A gestão destes factores de risco poder-se-á concentrar em aspectos como a redução de perdas, a melhoria da performance dos controlos internos, o desenvolvimento de uma cultura de risco operacional, ou o aumento do conhecimento interno da instituição e dos seus processos. As respostas obtidas das diferentes instituições que colaboraram neste estudo também demonstram a visão objectiva que estas possuem sobre a utilização da gestão de risco operacional como fonte de melhoria interna, com a banca a focar a sua atenção na minimização de perdas, na melhoria dos processos e serviços prestados aos clientes, e as seguradoras revelando uma maior preocupação com a sua imagem no mercado, com a melhoria dos seus processos e o desenvolvimento interno de uma cultura de risco.

Seja por pressões regulamentares, seja por as instituições já se terem apercebido da necessidade de reduzir a sua exposição a perdas operacionais, hoje, na sua maioria, as instituições financeiras já estão a desenvolver internamente áreas para a definição de

políticas e processos para a gestão de risco operacional. Com esse objectivo, e reconhecendo a necessidade de apoiar a sua actividade em informação e metodologias que lhes assegurem elevados padrões de eficácia e qualidade, as diferentes instituições encontram-se a implementar ou a desenvolver sistemas de informação para a gestão de risco operacional – na banca, todas as instituições contactadas dispõem já de um sistema de informação para risco operacional; nas seguradoras, a difusão destes sistemas ainda não é tão abrangente. A importância destes sistemas de informação é igualmente reconhecida pelas entidades de supervisão, que vêem na existência destes sistemas um alicerce vital na estrutura de gestão de risco operacional das instituições que supervisionam.

Estes sistemas de informação têm vindo a ser implementados com o objectivo primário de capacitar as instituições com informação necessária para responder aos requisitos dos supervisores (um dos objectivos primários tanto para bancos quanto para seguradoras). Nesse sentido, as funcionalidades requeridas pela maioria das instituições são, numa primeira fase, as que permitem fornecer essa mesma informação. Assim, na sua maioria, as instituições têm centrado as funcionalidades dos seus sistemas de informação na recolha de dados e na construção da sua base de dados de risco operacional. Para tal, têm enfrentado fortes desafios, dos quais se destacam a necessidade de integração do sistema com outras aplicações da instituição para recolha de dados e a dificuldade em garantir a aderência dos colaboradores ao programa de gestão de risco operacional e ao processo de recolha de informação de eventos, questionários ou indicadores de risco. No topo de todos os desafios, encontra-se a capacidade de assimilação, por parte de toda a instituição, da necessidade e mais-valias do programa de gestão de risco operacional – factor-chave para o sucesso do programa e para tornar a gestão de risco operacional em algo mais do que uma resposta a requisitos

regulamentares. A implementação de sistemas de informação poderá vir a representar um forte vector para contribuir para que as instituições financeiras portuguesas possam ter mecanismos de processamento de dados e disponibilização de conhecimento que as ajude a disseminar melhor os conceitos de gestão de risco operacional, contribuindo, deste modo, para auxiliar na captação de apoio e colaboração de todos os níveis da instituição.

Todavia, apesar de todas as dificuldades e desafios identificados, as diferentes instituições perceberam que, uma vez desenvolvida a base do programa de gestão de risco operacional e de um sistema de informação para o suportar e responder ao supervisor, o desenho de novas funcionalidades irá criar um novo conjunto de informação que permitirá mais-valias, tais como a redução de perdas e custos operacionais, a melhoria em processos, serviços, produtos, na imagem para o mercado e mesmo em aspectos mais indirectos como o nível de satisfação dos seus colaboradores.

Em Portugal, a implementação de sistemas de informação para gestão de risco operacional ainda é um processo com poucos anos de experiência; na sua totalidade, as instituições estão a segmentar a sua actividade de implementação, seja por falta de recursos humanos ou financeiros, seja por ainda existir alguma desconfiança sobre os reais benefícios de sistemas mais evoluídos e complexos. No estudo apresentado, ficou claro, no entanto, que a necessidade de um sistema de informação é vital e que as instituições portuguesas estão já a pensar em como potenciar a informação que podem recolher de forma a melhorarem aspectos internos ou a sua imagem no mercado. Os futuros sistemas de informação para risco operacional deverão ser mais do que apenas instrumentos para responder a requisitos de reguladores, deverão tornar-se ferramentas fundamentais para o processo estratégico e para as actividades operacionais das instituições financeiras. Para o efeito, estes sistemas deverão ter um conjunto de

funcionalidades que lhes permitam aceder a todo um conjunto de informação e tratá-lo, criando um conjunto de conhecimento que possa ser integrado na actividade das instituições, potenciando a melhoria em mecanismos que as protejam e ao mercado, ao mesmo tempo em que as tornam mais eficientes e rentáveis. Estas funcionalidades deverão responder a quatro grandes vectores: o processamento de dados; a descoberta de padrões e comportamentos; a capacidade de produzir informação que permita à instituição melhorar os seus processos internos e a qualidade dos seus serviços e a capacidade de disseminar uma cultura de risco dentro da instituição.

Com o estudo apresentado, o autor pretende contribuir para o desenvolvimento do conhecimento em dois eixos fundamentais: no primeiro, mais prático, pretendeu-se sistematizar a informação de como as instituições financeiras em Portugal estão a abordar o tema risco operacional e vêem a importância dos sistemas de informação, e da sua utilização, na gestão de risco operacional. Foi, igualmente, demonstrada a elevada relevância que as entidades supervisoras conferem a este tema. Com a apresentação de uma nova arquitectura de sistema de informação, o autor tencionou estabelecer linhas orientadoras para que as instituições financeiras possam evoluir para sistemas de informação com funcionalidades mais sofisticadas e, com estas, potenciar o desenvolvimento das suas capacidades de gestão de risco operacional, melhorando, assim, os seus resultados e a sua vertente organizacional, tanto interna quanto externa.

No segundo eixo, o autor quis apresentar, com este trabalho, vectores para o desenvolvimento do estudo académico dos sistemas de informação para a gestão de risco operacional. Sendo esta uma área em que o trabalho académico ainda é reduzido – o enfoque reside nas metodologias de gestão ou em análises estatísticas e econométricas –, é importante que se comece a abordar e a estudar o efeito que os sistemas de informação incutem na gestão de um dos riscos que mais impacto têm no

funcionamento e nos resultados das instituições financeiras. Este trabalho apresenta uma primeira sistematização do conhecimento sobre os sistemas de informação para risco operacional em instituições financeiras em Portugal e poderá constituir a base para futuros estudos sobre os impactos e a evolução do risco operacional no nosso país. A arquitectura exposta pretende configurar uma proposta na qual futuros investigadores se possam basear para o desenvolvimento de novos sistemas de informação, ou para ser utilizada no crescimento de novos paradigmas e metodologias de gestão de risco operacional.

O risco operacional afecta directa ou indirectamente os resultados das instituições financeiras, por conseguinte, é determinante identificar fontes e tipos de risco, quais são os níveis correntes de perdas, como mitigar o risco, como incentivar uma boa gestão de risco e quais os níveis de capital a alocar. A gestão de risco operacional deve ser incorporada na cultura organizacional, através quer da definição dos níveis de "apetite" ao risco da instituição (e.g. número e impacto de cada categoria de risco), como uma métrica que apoie o processo de decisão relativamente a opções sobre como actuar perante oportunidades ou ameaças identificadas, quer da evolução do conceito de gestão de risco operacional – que envolve desde um programa para identificar e reduzir perdas, até um programa para aumentar o conhecimento interno da instituição, de forma a utilizá-lo como uma fonte de criação de valor e de desenvolvimento de capacidades internas que permita a expansão dessa instituição dentro dos mercados onde actua ou pretende actuar. De futuro, cada decisão ou acção, independentemente do investimento associado, deve compreender uma revisão explícita do risco operacional envolvido, dos níveis de exposição previstos e dos mecanismos de mitigação disponíveis (e.g. uma mudança num processo que impactos pode ter em novos riscos, na mitigação dos existentes, impactos noutros processos, necessidade de novos controlos, etc.). Ao longo

do tempo, dever-se-á tornar uma parte integrante de cada processo de tomada de decisão dentro da instituição.

8 – INVESTIGAÇÃO FUTURA

Só recentemente os bancos e as seguradoras começaram a desenvolver os seus programas de gestão de risco operacional e a implementar sistemas de informação para os suportar. Tendo sido as imposições regulamentares a pressionar este desenvolvimento, a maioria das instituições financeiras centrou-se, na primeira fase, no cumprimento daqueles que são os requisitos dos seus supervisores. Assim sendo, actualmente a investigação só se poderá concentrar em questões como: razões pelas quais as instituições financeiras avançam para a gestão de risco operacional; o formato da implementação de sistemas de informação que a suportem e quais as funcionalidades que esperam ver nestes reflectidas. Ao mesmo tempo, podemos compreender o que estas instituições esperam que sejam os desafios e as mais-valias da gestão de risco operacional. Ou seja, a investigação actual aborda os primeiros passos das instituições no desenvolvimento da gestão de risco operacional e inquire sobre quais são as expectativas destas instituições para o futuro da gestão e dos sistemas de risco operacional.

A própria evolução dos programas de gestão de risco operacional nas instituições vai provocar novos desenvolvimentos e requisitos nos sistemas de informação. É também de esperar que este novo processo de gestão venha a ter implicações na forma como as instituições operam as suas actividades diárias e definem a sua estratégia. Com este amadurecimento, nova investigação será possível e necessária e deverá cobrir tópicos como: necessidade de implementações para fazer face a alguns dos desafios que

se colocam ao desenvolvimento da gestão de risco operacional nas instituições; ou o real impacto deste processo de gestão nos resultados das instituições. De seguida, são apresentados alguns destes tópicos para investigação futura:

1. Integração de dados – no caso de um grupo económico em que exista mais do que uma instituição, e no caso em que sejam de sectores diferentes (e.g. um banco e uma seguradora), a capacidade de agregar os dados que são fornecidos pelas diferentes instituições será vital não só para que se consiga desenvolver uma visão global da exposição do grupo a risco operacional, como também para analisar o seu perfil de risco e potenciais medidas de mitigação. Esta integração irá permitir um aumento do nível de conhecimento das instituições, ao mesmo tempo em que pode desenvolver sinergias, medidas de mitigação e de controlo interno conjuntas;
2. Integração da informação produzida pelo sistema de risco operacional nos processos de negócio das instituições – como foi referido em diversas situações, a integração do sistema de risco operacional com outros sistemas das instituições tem sido realizada essencialmente num sentido único, ou seja, diferentes sistemas da instituição têm enviado informação para o sistema de risco operacional. A informação que a gestão de risco operacional tem capacidade de fornecer tornar-se-á tanto mais importante quanto maior for a capacidade de cada instituição para a utilizar nos seus processos diários de negócio. A forma como essa integração deverá ser realizada (metodologias, forma e conteúdos) carece de investigação que permita que esta informação potencie melhorias quantitativas e qualitativas no modo como os processos das instituições são implementados;

3. Modelação de dados – esta é uma área em que, apesar de ter sido desenvolvido inúmero trabalho académico para a suportar, ainda existe a falta de evidências práticas sobre quais as melhores técnicas e metodologias para a modelação de risco operacional, por exemplo, como estimar a severidade para eventos de quantificação mais complexa ou a alocação de custos indirectos. Outro aspecto que deverá ser alvo de investigação futura é a criação dos alicerces para que seja possível comprovar a ligação entre risco de crédito e risco operacional (algo que já está previsto no acordo Basileia II), de forma a reduzir o nível de capital a alocar. Um tópico relevante na área de modelação assenta na capacidade de utilizar técnicas de *data mining* com o objectivo de auxiliar as instituições na detecção de factores de risco mais significativos e a obter informação sobre padrões e seus comportamentos que as ajude a explicar os seus eventos, níveis de exposição ao risco, bem como a encontrar as medidas de mitigação mais eficientes para cada tipo de risco operacional;
4. Reporte de informação – a futura investigação também deverá concentrar a sua atenção no desenho dos modelos de como deverão ser apresentados os relatórios de risco operacional à organização, no que concerne à sua forma e conteúdo. Esta questão irá ter um enorme impacto em dois factores essenciais na gestão de risco operacional: no desenvolvimento e assimilação da cultura de risco operacional por toda a organização e na capacidade de a gestão analisar e tomar decisões que permitam reduzir a exposição da instituição ao risco operacional.

Existe uma área de investigação mais global onde será urgente concentrar esforços dentro de um período de tempo médio (entre um a dois anos), após as instituições financeiras terem implementado os seus sistemas de informação. Será de extrema

importância investigar qual foi o impacto da implementação da gestão de risco operacional e dos seus sistemas de informação dentro de cada uma destas instituições. Analisar se existiram mudanças na cultura, na forma como o negócio é planeado e concretizado; analisar impactos financeiros, tais como a redução do nível de perdas; analisar se existem diferenças na imagem que a empresa detém no mercado, na optimização de recursos, ou em aspectos mais qualitativos, como o impacto registado na qualidade dos serviços que são prestados aos clientes – a investigação de todos estes tópicos irá permitir o desenvolvimento do conhecimento na área de risco operacional e ajudar a solidificar uma área de investigação que, apesar de já não ser embrionária, ainda não se encontra no nível de solidez académica e empresarial que se verifica para as áreas do risco de mercado ou do risco de crédito.

VII PARTE – APÊNDICES

Com os objectivos de perceber como as instituições financeiras estão a abordar a gestão de risco operacional e qual o papel dos sistemas de informação nestes programas, bem como a visão dos supervisores sobre estes dois temas, foram desenvolvidos questionários para facilitar a comunicação entre o autor e os interlocutores de cada uma das instituições consultadas. Foram construídos dois tipos de questionários (conjunto de questões semiabertas): um para as instituições financeiras e outro para as duas entidades reguladoras; os questionários foram preparados com base na revisão de literatura, num conjunto de entrevistas realizadas no início deste trabalho junto das instituições, para recolher dados sobre a sua aderência à gestão de risco operacional, e nos dados recolhidos em projectos nacionais de implementação de sistemas de informação para a gestão de risco.

Foi identificado um conjunto de instituições com capacidade, à data da realização desta investigação, para responder ao questionário. Numa primeira fase, foram contactadas para que lhes fosse explicado o objectivo da investigação, para saber da sua disponibilidade para nela participarem e, em caso afirmativo, para identificar os elementos que participariam no questionário – essencialmente, os responsáveis pelas áreas de gestão de risco operacional e elementos dos departamentos de sistemas de informação. Numa segunda fase, para as instituições que aderiram a este estudo, as entrevistas foram executadas de acordo com dois processos: no caso de haver disponibilidade por parte dos entrevistados, o questionário foi levado a cabo de forma presencial; nos restantes casos, este foi enviado por correio electrónico e as respostas foram obtidas usando o mesmo método – em caso de necessidade de esclarecimento de alguma dúvida nas respostas, procedeu-se da mesma forma. Em ambos os processos, foram identificadas vantagens e desvantagens. No caso da realização presencial, foi mais fácil explicar os objectivos e garantir respostas mais direccionadas para o tópico de

cada questão; no entanto, a liberdade natural deste contacto pessoal também implicou situações de respostas vastas e de mais difícil sistematização; situação que, no caso do segundo processo, não se verificou, tendo as instituições contactadas por correio electrónico apresentado respostas estruturadas em listas de itens, o que facilitou a sua sistematização. Houve, porém, situações em que foi mais difícil passar o contexto que se pretendia para cada uma das questões. Apresentam-se, de seguida, os dois questionários utilizados nesta investigação

Questionário para tese de doutoramento em Sistemas de Informação para Risco Operacional em Instituições Financeiras enviado às instituições financeiras:

1 – Quais os objectivos da gestão do risco operacional na sua instituição?

2 – Requisitos regulamentares:

2.1 – Qual a abordagem regulamentar que têm implementada actualmente?

2.2 – Qual a abordagem regulamentar que pretendem seguir?

3 – Qual a estrutura de gestão de risco operacional implementada ou a implementar?

4 – Sistemas de informação:

4.1 – Existe um sistema de informação para risco operacional na instituição?

4.2 – Se sim:

4.2.1 – Quais as funcionalidades base do sistema?

4.2.2 – Quais as fontes de dados que o alimentam?

4.2.3 – Quais os métodos de cálculo que vão ser utilizados para requisitos de capital?

4.2.4 – Vê outros tipos de análises como importantes além dos cálculos de requisito de capital? Quais?

4.2.5 – Tipo de reporte disponibilizado?

4.2.6 – Qual é o número de utilizadores estimado dos sistemas?

5 – Como vê a evolução da gestão de risco operacional na sua organização?

5.1 – Quais os grandes desafios?

5.2 – Quais as mais-valias de uma gestão do risco operacional?

6 – Quais as características / funcionalidades que acha importantes que um sistema de risco operacional possua além das que enunciou no ponto 4.2.1?

Questionário para tese de doutoramento em Sistemas de Informação para Risco Operacional em Instituições Financeiras enviado às entidades reguladoras:

1– Como vê a entidade reguladora a gestão de risco operacional nas diferentes instituições?

2 – Qual a abordagem regulamentar que prevê que as instituições irão seguir?

3 – Qual a importância que a entidade reguladora irá dar à existência de um sistema de informação para a gestão de risco operacional?

4 – Quais as funcionalidades base que vê com maior importância neste tipo de sistemas?

5 – Como vê a evolução da gestão de risco operacional nas diferentes instituições?

5.1 – Quais os grandes desafios?

5.2 – Quais as mais-valias de uma gestão do risco operacional para a entidade reguladora?

VIII PARTE – REVISÃO BIBLIOGRÁFIA

9 - BIBLIOGRAFIA

Alexander, C. (2003). “Managing Operational Risks with Bayesian Networks.” Pp. 285–294 in *Operational Risk: Regulation, Analysis and Management*, ed. C. Alexander. London: Prentice Hall-Financial Times.

Alexander, C. (2003). “Statistical Models of the Operational Loss.” Pp. 129–170 in *Operational Risk: Regulation, Analysis and Management*, ed. C. Alexander. London: Prentice Hall-Financial Times.

Alexander, C. (Ed.). (2001). *Mastering risk – volume 2: Applications*. London: Pearson Education.

Alexander, C. (Ed.). (2003). *Operational Risk – Regulation, Analysis and Management*. London: Pearson Education.

Alexander, C. (2004). *The Present and Future of Financial Risk Management*, http://jfec.oupjournals.org/cgi/content/abstract/3/1/3

Allen, L. & Bali, T. G. (2004). “Cyclicality in Catastrophic and Operational Risk Measurements.” Working Paper, City University of New York, September.

Allen, L. & Turan, G. B. (2007). “Cyclicality in Catastrophic and Operational Risk Management.” *Journal of Banking and Finance* 31: 1191–1235.

Altman, E. & Saunders, A. (2001). “Credit Ratings and the BIS Reform Agenda.” Unpublished paper, New York University.

Andres, U. & Brink, G. J. Van Der. (2004). “Implementing a Basel II Scenario-Based AMA for Operational Risk.” Pp. 343–368 in *The Basel Handbook*, ed. K. Ong. London: Risk Books.

Barth, J., Caprio, G. & Levine, R. (2006). *Rethinking Bank Regulation: Till Angels Govern*. New York: Cambridge University Press.

Basel Committee on Banking Supervision [BCBS]. (2003). *Basel II Acord*, www.bis.org.

BCBS. (2001). *Basel II: The New Basel Capital Accord-Second Consultative Paper*. Basel: Bank for International Settlements, www.bis.org.

BCBS. (2001). *Operational Risk: Supporting Document to the New Basel Accord*. Basel: Bank for International Settlements.

BCBS. (2001). *Working Paper on the Regulatory Treatment of Operational Risk*. Basel: Bank for International Settlements.

BCBS. (2003). *Operational Risk Transfer Across Financial Sectors*. Basel: Bank for International Settlements.

BCBS. (2003). *Sound Practices for the Management of Operational Risk*. Basel: Bank for International Settlements.

BCBS. (2003). *Supervisory Guidance on Operational Risk: Advanced Measurement Approaches for Regulatory Capital*. Basel: Bank for International Settlements.

BCBS. (2003). *The 2002 Data Collection Exercise for Operational Risk: Summary of the Data Collected*. Basel: Bank for International Settlements.

BCBS. (2004). *Bank Failures in Mature Economies*. Basel: Bank for International Settlements.

BCBS. (2004). *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework*. Basel: Bank for International Settlements.

Bee, M. (2005). "Copula-Based Multivariate Models with Applications to Risk Management and Insurance." Unpublished paper, Università degli Studi di Trento.

Bee, M. (2006). "Estimating the Parameters in the Loss Distribution Approach: How can we Deal with Truncated Data?" Pp. 123–144 in *The Advanced Measurement Approach to Operational Risk*, ed. E. Davis. London: Risk Books.

Benston, G. J. & Kaufman, G. G. (1996). "The Appropriate Role of Bank Regulation." *Economic Journal* 106: 688–697.

Bessis, J. (2002). *Risk Management in Banking* (2nd. edition). West Sussex: John Wiley & Sons.

Bhatia, M. (2002). "New Basel Accord: Operational Risk Management – Emerging Frontiers for the Profession." *Information Systems and Control Journal*, www.isaca.org.

Bilby, R. (2008). "Using Scenario Analysis to Achieve Sound Operational Risk Management". Paper Presented at the OpRisk Asia Conference, Singapore 2–4.

Blunden, T. (2003). "Scoreboard Approaches." Pp. 229–240 in *Operational Risk: Regulation, Analysis and Management*, ed. C. Alexander. London: Prentice Hall-Financial Times.

Bocker, K. & Kluppelberg, C. (2005). "Operational VAR: A Closed-Form Approximation." *Risk* December: 90–93.

Bolton, N. & Berkey, J. (2005). "Aligning Basel II Operational Risk and Sarbanes-Oxley 404 Projects." Pp. 237–246 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Brandts, S. (2005). "Reducing Risk Through Insurance." Pp. 305–314 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Brink, Gerrit J. Van Der. (2002). *Operational Risk: The new challenge for banks*. Palgrave Publishers.

Buchelt, R. & Unteregger, S. (2004). "Cultural Risk and Risk Culture: Operational Risk after Basel II, Financial Stability Report 6." http://www.oenb.at/en/img/fsr 06 cultural risk tcm16–9495.pdf.

Cagan, P. (2001). "Seizing the Tail of the Dragon." *FOW/Operational Risk* July: 18-23.

Cagan, P. (2005). "External Data: Reaching for the Truth", www.operationalriskonline.com.

Chapelle, A., Crama, Y., Hubner, G. & Peters, J. P. (2004). "Basel II and Operational Risk: Implications for Risk Measurement and Management in the Financial Sector." Unpublished paper, National Bank of Belgium. *Operational Risk: A Survey* 195.

Chernobai, A. & Rachev, S. (2004). "Stable Modelling of Operational Risk." Pp. 139–170 in *Operational Risk Modelling and Analysis*, ed. M. Cruz. London: Risk Books.

Chernobai, A., Menn, C., Rachev, S. T., Truck, S. & Moscadelli, M. (2006). "Treatment of Incomplete Data in the Field of Operational Risk: The Effects on Parameter Estimates, EL and UL Figures." Pp. 145–468 in *The Advanced Measurement Approach to Operational Risk*, ed. E. Davis. London: Risk Books.

Chorafas, Dimitris N. (2001). *Managing Operational Risk: Risk reduction strategies for investment and commercial banks.* Euromoney Books.

Commonwealth Bank of Australia. (1999). *Annual Report*. Sydney: Commonwealth Bank of Australia.

Consiglio, A. S. A. Zenios. (2003). "Model Error in Enterprise-wide Risk Management: Insurance Policies with Guarantees." Pp. 179–196 in *Advances in Operational Risk: Firm-wide Issues for Financial Institutions* (2nd. edition). London: Risk Books.

Crouchy, M. (2001). *Risk Management*. New York: McGraw Hill.

Crouchy, M., Galai, D. & Mark, R. (2004). "Insuring versus Self-Insuring Operational Risk: Viewpoints of Deposits and Shareholders." *Journal of Derivatives* 12: 51–55.

Crouchy, M., Galai, D. & Mark, R. (1998). "Key Steps in Building Consistent Operational Risk Management and Measurement." Pp. 45–62 in *Operational Risk and Financial Institutions*. London: Risk Books.

Cruz, M. (2002). *Modelling, Measuring and Hedging Operational Risk*. New York: Wiley.

Cruz, M. (2003). "Operational Risk: Past, Present and Future." Pp. 271–286 in *Modern Risk Management: A History*, ed. P. Field. London: Risk Books.

Cummins, J. D., Lewis, C. M. & Wei, R. (2006). "The Market Value Impact of Operational Loss Events for US Banks and Insurers." *Journal of Banking and Finance* 30: 2605–2634.

Currie, C. V. (2004). "Basel II and Operational Risk: An Overview." Pp. 271–286 in *Operational Risk Modelling and Analysis*, ed. M. Cruz. London: Risk Books.

Currie, C. V. (2006). "A Test of the Strategic Effect of Basel II Operational Risk Requirements on Banks." *ICFAI Journal of Monetary Economic*, 4, 6-28.

Danielsson, J. & Zigrand, J. P. (2003). "What Happens when You Regulate Risk? Evidence from a Simple Equilibrium Model." Unpublished paper, London School of Economics.

Danielsson, J. (2003). "On the Feasibility of Risk Based Regulation." Unpublished paper, London School of Economics.

Danielsson, J., Embrechts, P., Goodhart, C., Keating, C., Muennich, F., Renault, O. & Shin, H. S. (2001). "An Academic Response to Basel II." Unpublished paper, LSE Financial Markets Group.

Danielsson, J., Shin, H. S. & Zigrand, J. P. (2002). "The Impact of Risk Regulation on Price Dynamics." Unpublished paper, London School of Economics.

Davis, E. (2005). "Loss Data Collection and Modelling." Pp. 1–2 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Davis, J., Finlay, M., McLenaghen, T. & Wilson, D. (2006). "Key Risk Indicators – Their Role in Operational Risk Management and Measurement." Pp. 215–245 in *The Advanced Measurement Approach to Operational Risk*, ed. E. Davis. London: Risk Books.

de Fontnouvelle, P., DeJesus-Rueff, V., Jordan, John S. & Rosengren, Eric S. (2006). "Capital and Risk: New Evidence on Implications of Large Operational Losses." *Journal of Money, Credit, and Banking* 38: 1819-1846.

de Fontnouvelle, P., Rosengren, E. & Jordan, J. (2004). "Implications of Alternative Operational Risk Modelling Techniques." Unpublished paper, Federal Reserve Bank of Boston.

de Koker, R. (2006). "Operational Risk Modelling: Where Do we Go from Here?" *The Advanced Measurement Approach to Operational Risk*, ed. E. Davis. London: Risk Books.

Dickstein, Dennis I. & Flast, Robert H. (2009). "No excuses – A Business Process Approach to Managing Operational Risk". New Jersey: John Wiley & Sons.

Doerig, H. U. (2003). Operational Risks in Financial Services: An Old Challenge in a New Environment. Working Paper. Credit Suisse Group.

Dowd, V. (2003). “Measurement of Operational Risk: The Basel Approach.” Pp. 31–48 in *Operational Risk: Regulation, Analysis and Management*, ed. C. Alexander. London: Prentice Hall-Financial Times.

Economist, The. (2003). “Deep Impact.” *The Economist* 8 May.

Embrechts, P., Lindskog, F. & McNeil, A. (2003). “Modelling Dependence with Copulas and Applications to Risk Management.” Pp. 329–384 in *Handbook of Heavy Tailed Distributions in Finance*, ed. S. Rachev. Amsterdam: Elseiver.

Fama, E. F. K. French. (1993). “Common Risk Factors in the Returns on Stocks and Bonds.” *Journal of Financial Economics* 33: 3–56.

Fitch Ratings. (2004). “Operational risk management & Basel II implementation: Survey results.”

Frachot, A. & Roncalli, T. (2002). “Mixing Internal and External Data for Managing Operational Risk.” Unpublished paper, Credit Lyonnais.

Frachot, A., Moudoulaud, O. & Roncalli, T. (2004). “Loss Distribution Approach in Practice” in *The Basel Handbook*, ed. K. Ong. London: Risk Books.

Frachot, A., Roncalli, T. & Salmon, E. (2004). “The Correlation Problem in Operational Risk.” Working Paper, Credit Lyonnais.

Fujii, K. (2005). “Building Scenarios.” Pp. 169–178 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Geiger, Hans. (2002). “Regulation and Supervising Operational Risks for Banks” in conference “Future of Financial Regulation: Global Regulatory Reform and Implications for Japan.”

Gelderman, M., Klaassen, P. & Lelyveld, I. van. (2006). “Economic Capital: An Overview.” Pp. 1–12 in *Economic Capital Modelling: Concepts, Measurement and Implementation*, ed. I. van. Lelyveld. London: Risk Books.

Gibson, Michael S. (1997). *Information Systems for Risk Management*, www.bog.frb.fed.us.

Giraud, J. R. (2005). "Managing Hedge Funds' Exposure to Operational Risks." Pp. in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Giudici, P. & Bilotta, A. (2004). "Modelling Operational Losses: A Bayesian Approach." *Quality and Reliability Engineering International* 20:407–417.

Giudici, P. (2004). "Integration of Qualitative and Quantitative Operational Risk Data: A Bayesian Approach." Pp. 131–138 in *Operational Risk Modelling and Analysis: Theory and Practice*, ed. M Cruz. London: Risk Books.

Grinsven, J.H.M., Bloemkolk, R. (2009). "Solvency II: Dealing with Operational Risk", *FSI Magazine*.

Group of Thirty (1993). *Derivatives: Practices and Principles*. Washington DC: Group of Thirty.

Haas, M. & Kaiser, T. (2004). "Tackling the Inefficiency of Loss Data for the Quantification of Operational Loss." Pp. 13–24 in *Operational Risk Modelling and Analysis: Theory and Practice*, ed. M. Cruz. London: Risk Books.

Hadjiemmanuil, C. (2003). "Legal Risk and Fraud: Capital Charges, Control and Insurance." Pp. 74–100 in *Operational Risk: Regulation, Analysis and Management*, ed. C. Alexander. London: Prentice Hall-Financial Times. *Operational Risk: A Survey*.

Halperin, K. (2001). "Balancing Act." *Bank Systems and Technology* 38: 22–25.

Haubenstock, M. & Hardin, L. (2003). "The Loss Distribution Approach." Pp. 171–192 in *Operational Risk: Regulation, Analysis and Management*, ed. C. Alexander. London: Prentice Hall-Financial Times.

Haubenstock, M. & Hause, J. (2006). "Practical Decisions to Successfully Model Operational Risk Capital" Pp. 15–36 in *The Advanced Measurement Approach to Operational Risk,* ed. Ellen Davis. London: Risk Books.

Helbok, Gunther & Wagner, Christian. (2006). "Determinants of Operational Risk Reporting in the Banking Industry." *Journal of Risk.*

Herring, R. J. (2002). "The Basel 2 Approach to Bank Operational Risk: Regulation on the Wrong Track." Unpublished paper, University of Pennsylvania.

Hoffman, D. G. (1998). "New Trends in Operational Risk Measurement and Management." Pp. 29–44 in *Operational Risk and Financial Institutions*. London: Risk Books.

Hoffman, D. G. (2002). *Managing operational risk.* New York: John Wiley & Sons.

Holmes, M. (2003). "Measuring Operational Risk: A Reality Check." *Risk* 16: 84–87.

Hubbard, Douglas W. (2009). *The Failure of Risk Management*. New Jersey: John Wiley & Sons.

Hubner, R., Laycock, M. & Peemoller, F. (2003). "Managing Operational Risk." Pp. in *Advances in Operational Risk: Firm-wide Issues for Financial Institutions*. London: Risk Books.

Hughes, P. (2005). "Using Transaction Data to Measure Operational Risk." Pp. 3–12 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Institute of Operational Risk. (2010). "Risk Control Self-Assessment".

Jameson, R. (1998). "Playing the Name Game." *Risk* 11: 38–42.

Jobst, Andreas A. (2007). "Consistent Quantitative Operational Risk Measurement and Regulation: Challenges of Model Specification, Data Collection and Loss Reporting", IMF Working Paper.

Kahneman, D.,Tversky, A. (1972). "Subjective Probability: A Judgment of Representativeness" in *Cognitive Psychology* 3: 430-454.

Kaiser, T. & Kohne, M. (2006). *An Introduction to Operational Risk*. London: Risk Books.

Kalhoff, Agatha & Hass, Marcus. (2004). "Operational Risk – Management Based on the Current Loss Data Situation", in *Operational Risk Modeling and Analysis – Theory and Practice*, ed. Marcelo Cruz. Incisive Media Investments Limited.

Kalyvas, L. & Sfetsos, A. (2006). "Does the Application of Innovative Internal Models Diminish Regulatory Capital?" *International Journal of Theoretical and Applied Finance* 9: 217–226.

Kalyvas, L., Akkizidis, I., Zourka, I. & Bouchereau, V. (2006). *Integrating Market, Credit and Operational Risk: A Complete Guide for Bankers and Risk Professionals*. London: Risk Books.

Kaufman, G. G. & Scott, K. (2000). "Does Bank Regulation Retard or Contribute to Systemic Risk?" Unpublished paper, Loyola University Chicago and Stanford Law School.

Kaufman, G. G. (2005) "Basel II vs Prompt Corrective Action: Which is the Best for Public Policy?" *Financial Markets, Institutions and Instruments* 14: 349-357.

Kennett, R. (2003). "How to Introduce an Effective Risk Management Framework." Pp. 73–94 in *Advances in Operational Risk: Firm-wide Issues for Financial Institutions* (2nd. edition). London: Risk Books.

Kingsley, S., Rolland, A., Tinney, A. & Holmes, P. (1998). "Operational Risk and Financial Institutions: Getting Started." Pp. 3–28 in *Operational Risk and Financial Institutions*. London: Risk Books.

Koehn, M. & Santomero, A. M. (1980). "Regulation of Bank Capital and Portfolio Risk." *Journal of Finance* 35: 1235–1244.

Koyuncugil, Ali S. & Ozgulbas, Nermin. (2008). "A Data Mining Model for Detecting Financial and Operational Risk Indicators of SMEs." *World Academy of Science, Engineering and Technology* 46: 88-91.

KPMG (2002). *Study into the methodologies to assess the overall financial position of an insurance undertaking from the perspective of prudential supervision*, http://intranet.icea.es/solvencia/Documentos/KPMG%20solv%20final%20report-300402.pdf.

KPMG (2005). *Managing Operational Risk Beyond Basell II*. KPMG Financial Services.

Kross, W. K. (2009). "Integrating 'Management' into 'Oprisk Management" Pp. 249-288 in *Operation Risk Toward Basel III*, ed. Greg N. Gregoriou. New Jersey: John Wiley & Sons.

Kuhn, R. & Neu, P. (2005). "Functional Correlation Approach to Operational Risk in Banking Organizations." Unpublished paper, Dresdner Bank AG.

Kuhn, R. & Neu, P. (2004). "Adequate Capital and Stress Testing for Operational Risk." Pp. 273–292 in *Operational Risk Modelling and Analysis*, ed. M. Cruz. London: Risk Books.

Lam, J. (2003). "A Unified Management and Capital Framework for Operational Risk." *RMA Journal* 58: 26.

Levine, R. S. (2007). *Implementing Systems Solutions for Financial Risk Management*. Risk Books.

Lewellyn, D. T. (Ed.). (2001). *Bumps on the Road to Basel: An Anthology of Basel 2*. London: Centre for the Study of Financial Innovation.

Lewis, C. M. & Lantsman, Y. (2005). What is a Fair Price to Transfer the Risk of Unauthorised Trading? A Case Study on Operational Risk." Pp. 315–356 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Lopez, J. A. (2002). "What is Operational Risk?" *Federal Reserve Bank of San Francisco Economic Letter* January.

Lopez, J. A. (2003). "Disclosure as a Supervisory Tool: Pillar 3 of Basel II", *Federal Reserve Bank of San Francisco Economic Letter* August.

Marshall, C. (2001). "Measuring and Managing Operational Risks in financial institutions." *Tools, Techniques and Other Resources*. John Wiley & Sons.

McConnel, P. (2008). "Operational Risk Capital under Basel II – Dead on Arrival?" www.riskmagazine.com.au.

Medova, E. A. & Kyriacou, M. N. (2001). "Extremes in Operational Risk Management." Unpublished paper, University of Cambridge.

Medova, E. A. (2002). "Operational Risk, Capital Allocation and Integration of Risks", http://www-cfr.jims.cam.ac.uk/archive/PAPERS/2001/WP10.pdf (23 de Julho 2004).

Mestchian, P. (2003). "Operational Risk Management: The Solution is in the Problem." Pp. 3–14 in *Advances in Operational Risk: Firm-wide Issues for Financial Institutions*. London: Risk Books.

Metcalfe, R. (2003). "Operational Risk: The Empiricists Strike Back." Pp. 435–446 in *Modern Risk Management: A History*, ed. P. Field. London: Risk Books.

Mignola, G. & Ugoccioni, R. (2007). "Effect of Data Collection Threshold in the Loss Distribution." *Journal of Operational Risk* 1 Winter: 35–47.

Milligan, J. (2004). "Prioritizing Operational Risk." *Banking Strategies* 80: 67.

Moody's Investor Service. (2003). "Moody's Analytical Framework for Operational Risk Management of Banks."

Moosa, I. A. (2007). "A Critique of the Advanced Measurement Approach to Regulatory Capital Against Operational Risk." Unpublished paper, Monash University.

Moosa, I. A. (2007). "Misconceptions about Operational Risk." *Journal of Operational Risk* Winter: 97–104.

Moosa, I. A. (2007). *Operational Risk Management*. London: Palgrave.

Moosa, I. A. (2007). *Operational Risk: A Survey*. New York University Salomnn Center, Financial Markets, Institutions & Instruments, V. 16. No.4.

Moosa, I. A. (2008). "Quantification of Operational Risk Under Basel II. The Good, Bad and Ugly." Financial and Capital Market Series, University of Reading.

Moscadelli, M. (2005). "The Modelling of Operational Risk: Experience with the Analysis of the Data collected by the Basel Committee." Pp. 39–106 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Moscadelli, M., Chernobai, A. & Rachev, S. (2005). "Treatment of Incomplete Data in the Field of Operational Risk: The Effects on Parameter Estimates, EL and UL Figures." *Operational Risk* June: 33–50.

Muzzy, L. (2003). "The Pitfalls of Gathering Operational Risk Data." *RMA Journal* 85: 58–62.

Na, H. S., Miranda, L. C., Berg, J. Van Den & Leipoldt, M. (2005). "Data Scaling for Operational Risk Modelling." *ERIM Report Series* ERS-2005–092-LIS, December.

Nash, Ralph A. (2003). "The three pillars of operational risk" in *Operational Risk: Regulation, Analysis and Management*, ed. Carol Alexander. Pearson Education Limited.

Netter, J. M. & Poulsen, A. B. (2003). "Operational Risk in Finance Service Providers and the Proposed Basel Capital Accord: An Overview", in *Advances in Financial Economics* 8, 147-172.

Ong, M. (2002). "The Alpha, Beta and Gamma of Operational Risk." *RMA Journal* 85: 34.

Parsley, M. (1996). "Risk Management's Final Frontier." *Euromoney* September: 74–75.

Peccia, A. (2003). "Using Operational Risk Models to Manage Operational Risk." Pp. 363–384 in *Operational Risk: Regulation, Analysis and Management*, ed. C. Alexander. London: Prentice Hall-Financial Times. *Operational Risk: A Survey* 199.

Peccia, A. (2004). "An Operational Risk Ratings Model Approach to Better Measurement and Management of Operational Risk." Pp. in *The Basel Handbook*, ed. K. Ong. London: Risk Books.

Pezier, J. (2003). "A Constructive Review of the Basel Proposals on Operational Risk." Pp. 49–73 in *Operational Risk: Regulation, Analysis and Management*, ed. C. Alexander. London: Prentice Hall-Financial Times.

Postlewaite, A. & Vives, X. (1987). "Bank Runs as an Equilibrium Phenomenon." *Journal of Political Economy* 95: 485–491.

Power, M. (2005). "The Invention of Operational Risk". *Review of International Political Economy* 12, 557-599.

Powojowski, M., Reynolds, D. & Tuenter, H. J. H. (2002). "Dependent Events and Operational Risk." *Algo Research Quarterly* 5: 65–73.

Raft International. (2002). *Emerging Trends in Operational Risk.*

Rao, V. & Dev, A. (2006). "Operational Risk: Some Issues in Basel II AMA Implementation in US Financial Institutions." Pp. 273–294 in *The Advanced Measurement Approach to Operational Risk*, ed. E. Davis. London: Risk Books.

Rebonato, R. (2007). "The Plight of the Fortune-Tellers: Thoughts on the Quantitative Measurement of Financial Risk." Unpublished manuscript.

Reisman, A. & Oral, M. (2004). *Soft Systems Methodology: A Context within a 50-year retrospective of OR/MS.*

Reynolds, D. & Syer, D. (2003). "A General Simulation Framework for Operational Loss Distributions." Pp. 193–214 in *Operational Risk: Regulation, Analysis and Management*, ed. C. Alexander. London: Prentice Hall-Financial Times.

Robert Morris Associates, British Bankers' Association and International Swaps and Derivatives Association. (1999). *Operational Risk: The Next Frontier*. Philadelphia: RMA.

Rosenberg, J. V. & Schuermann, T. (2006). "A General Approach to Integrated Risk Management with Skewed, Fat-Tailed Risks." *Journal of Financial Economics* 79: 569–614.

Rosengren, E. (2001). "Capital Allocation for Operational Risk – Implementation Challenges for Bank Supervisors." *Joint Operational Risk Conference.*

Saidenberg, M. & Schuermann, T. (2003). *The New Basel Capital Accord and Questions for Research*, http://fic.wharton.upenn.edu/fic/papers/03/0314.pdf.

Samad-Khan, A., Moncelet, B. & Pinch, T. (2006). "Uses and Misuses of Loss Data", www.opriskadvisory.com.

Sekaran, Uma. (2003). *Research methods for Business – A Skill Building Approach*. John Wiley & Sons, Inc.

Shadow Financial Regulatory Committee. (2001). "The Basel Committee's Revised Capital Accord Proposal." Statement No. 169, February.

Shepheard-Walwyn, & Litterman, T. R. (1998). "Building a Coherent Risk Measurement and Capital Optimisation Model for Financial Firms." *Federal Reserve Bank of New York Economic Policy Review* October: 171–182.

Smithson, C. & Song, P. (2004). "Quantifying Operational Risk." *Risk* July: 50–52.

Society of Actuaries. (2010). "A New Approach for Managing Operational Risk."

Sundmacher, M. (2007) "The Basic Indicators Approach and the Standardised Approach to Operational Risk: An Example and Case Study-Based Analysis." Ssrn.com/abstract=988282.

Swenson, Kenneth. (2003). *A Quantitative operational risk framework: guidance, structure and reporting*, ed. Carol Alexander. Pearson Education Limited.

Thirlwell, J. (2002). "Operational Risk: The Banks and the Regulators Struggle." *Balance Sheet* 10: 28–31.

Tripe, D. (2000). "Pricing Operational Risk." Unpublished paper, Massey University.

Turing, D. (2003). "The Legal and Regulatory View of Operational Risk." Pp. 253–266 in *Advances in Operational Risk: Firm-wide Issues for Financial Institutions* (2nd. edition). London: Risk Books.

Van Grinsven, J. & Bloemkolk, R. (2009). "Solvency II: Dealing with operational Risk" in *FSI magazine*.

Vinella, P. & Jin, J. (2005). "A Foundation for KPI and KRI." Pp. 157–168 in *Operational Risk: Practical Approaches to Implementation*, ed. E. Davis. London: Risk Books.

Wahler, B. (2002). "Process-Managing Operational Risk – Developing a Concept for Adapting Process Management to the Needs of Operational Risk in the Basel II-Framework", http://papers.ssrn.com/sol3/papers.cfm?abstract id=674221.

Watts, R. & Zimmerman, J. (1986). *Positive Accounting Theory*. London: Prentice Hall International.

Webb, A. (1999). "Controlling Operational Risk." *Derivatives Strategy* 4: 17–21.

Wei, R. (2003). "Operational Risk in the Insurance Industry." Unpublished paper, University of Pennsylvania.

Wei, R. (2006). *An Empirical* Investigation *of Operational Risk in the United States Financial Sectors*. University of Pennsylvania AAT 3211165.

Wei, R. (2007). "Quantification of Operational Losses Using Firm-Specific Information and External Databases." *Journal of Operational Risk* 1 Winter: 3–34.

Young, B & Coleman, R. (2009). *Operational risk assessment. A Commercial Imperative of a more Forensic and Transparent Approach.* Wiley Finance.

Young, B. & Ashby, S. (2003). "New Trends in Operational Risk Insurance for Banks." Pp. 43–58 in *Advances in Operational Risk: Firm-wide Issues for Financial Institutions* (2nd. edition). London: Risk Books.